JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. X No 1, Desember 2023, hlm. 171 - 178 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v10i1.2880
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

IDPS PERFORMANCE ANALYSIS FOR MITIGATING SQL INJECTIONS AND SYN FLOOD ATTACKS

Sahren[1*], Ruri Ashari Dalimunthe[1], Herman Saputra[1], Dian Yudha Kurnia Sirni[1]
[1]Sistem Komputer, Sekolah Tinggi Manajemen Informatika dan Komputer Royal
email: [*]sahren.one@gmail.com

Abstract: Cyberattacks like SQL injection and syn flood attacks can threaten the information system security of an organisation or company. The Intrusion Detection and Prevention System (IDPS) is used as a solution to detect, prevent, and respond to these attacks. However, the effectiveness of IDPS in protecting information systems needs to be evaluated through performance analysis. IDPS performance analysis for mitigating SQL injection and syn flood attacks will use Suricata tools, where performance analysis will include evaluation of system accuracy and efficiency in detecting attacks, as well as the impact of the system on network or information system performance. By doing this performance analysis, it can be seen how effective the IDPS is in providing defences against such attacks. The results of the IDPS performance analysis can help an organisation or company select and implement the right IDPS according to the needs and conditions of the information system. Thus, organisations or companies can improve the security of their information systems from threatening cyber attacks.

Keywords: IDPS; SQL_Injection; Suricata; Syn_Flood_Attack

Abstrak: Serangan cyber seperti SQL Injection dan Syn Flood Attack dapat mengancam keamanan sistem informasi suatu organisasi atau perusahaan. Intrusion Detection and Prevention System (IDPS) digunakan sebagai solusi untuk mendeteksi, mencegah, dan merespons serangan-serangan ini. Namun, efektivitas IDPS dalam melindungi sistem informasi perlu dievaluasi melalui analisis performa. Analisis performa IDPS untuk mitigasi SQL Injection dan Syn Flood Attack ini akan menggunakan tools suricata dimana analisa performa akan meliputi evaluasi terhadap akurasi dan efisiensi sistem dalam mendeteksi serangan, serta dampak dari sistem terhadap kinerja jaringan atau sistem informasi. Dengan melakukan analisis performa ini, dapat diketahui seberapa efektif IDPS dalam memberikan perlindungan terhadap serangan-serangan tersebut. Hasil dari analisis performa IDPS dapat membantu organisasi atau perusahaan dalam memilih dan mengimplementasikan IDPS yang tepat sesuai dengan kebutuhan dan kondisi sistem informasi yang dimiliki. Dengan demikian, organisasi atau perusahaan dapat meningkatkan keamanan sistem informasi mereka dari serangan-serangan cyber yang mengancam.

Kata kunci: IDPS; SQL_Injection; Suricata; Syn_Flood_Attack

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. X No 1, Desember 2023, hlm. 171 - 178 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v10i1.2880
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

INTRODUCTION

SQL injection and syn flood attacks belong to the types of cyber attacks that can damage the information systems of an organisation or company. [1]. SQL injection is done by inserting a malicious SQL command into the data input of an application, so it can take over or modify the data stored in the database. [2][3]. Meanwhile, the Syn Flood Attack is done by sending a large number of connection requests to the server, so the server can't handle the request and becomes unresponsive. [4][5].

To protect information systems from these attacks, intrusion detection and prevention systems are usually used. (IDPS) [6]. Where the tools are to be used is Suricata. IDPS is a security system designed to detect, prevent, and respond to attacks on a network or information system [7].

However, in the use of IDPS, it is necessary to perform performance analysis to ensure the effectiveness of the IDPS system in identifying and preventing SQL injection and Syn Flood Attack attacks [8][9]. This performance analysis includes an evaluation of the accuracy and efficiency of an attack-detecting system as well as an assessment of the impact of the system on network or information system performance [10].

F. Raditya and J. Sidabutar conducted previous research in 2020 [11], Analyzing the Suricata Intrusion Detection Prevention System (IDPS) Rules for detecting and preventing crypto mining activities on the network. During this research, we calculated accuracy, precision, recall, and f-measure values as part of the analysis. The results show that implementing the custom rule for detecting and mitigating crypto mining activities increases the accuracy value by 0.2%, the recall value by 48.94%, and the f-measure value by 32.39% compared to using the default rule, Suricata. Then, in 2022, research conducted by D. T. Yuwono and S. A. Nuswantoro [12], discussed the analysis and performance of intrusion detection systems in detecting cyber-attacks on Apache Web Server. In this research, we tested the performance of IDS in detecting flooding attacks on web servers, and the detection results were displayed in web form. Another study was conducted by E. H. Kalabo in 2022 [6], which discussed the performance analysis of the Snort and Suricata Intrusion Detection System (IDS) against TCP SYN Flood Attacks. This research produces a comparison of IDS performance using Snort and Suricata by looking at the accuracy, speed and RAM consumption values used by the IDS, while the form of attack tested is the SYN Flood Attack.

By conducting an IDPS performance analysis for mitigating SQL Injection and Syn Flood Attack, it can be seen how effective the IDPS system is in providing protection against such attacks. This can help organizations or companies in selecting and implementing the right IDPS according to the needs and conditions of the information system.

METHOD

Research methodology is a branch of science that explains how to do research, from searching for information to writing it down and analyzing it to putting together reports based on what the research found. The motivation and purpose of doing research in general are essentially the same: that research is a picture of human desire itself, which in

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. X No 1, Desember 2023, hlm. 171 - 178 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v10i1.2880
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

fact always wants to know something new in a particular field. The desire to acquire and update science becomes a fundamental need for every human being, which is generally the primary motivation when doing research.

This research methodology is conducted systematically and can be used as a guideline or reference for researchers when conducting research so that the results achieved do not deviate and the desired objectives can be implemented well, correctly and in accordance with what has been previously determined.

This research was carried out at STMIK Royal in the network laboratory, including activities in carrying out topology design, configuration, testing and collecting test data, which will be used as a reference for carrying out final analysis. The sequence of these activities is stated in the form of a research framework. The framework of the research covers the systematic stages carried out by the author in completing the research related to the IDPS Performance Analysis for Mitigating SQL Injection and Syn Flood Attack used, as shown in Image 1.

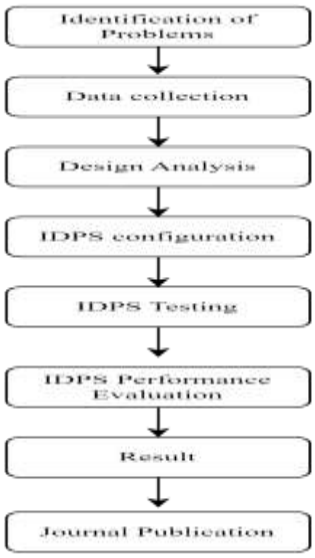

Image 1. Research Framework

Identification This problem will result in the identification of system requirements, including the type of attack to be encountered, available system resources, and network usage requirements. Identifying system needs will help determine which type of IDPS is most suitable for implementation.

Design analysis involves selecting the type of IDPS that best suits system requirements and follows established security standards. There are several types of IDPS that you can choose from, such as network-based, host-based or hybrid IDPS. Each type has its advantages and disadvantages, so the selection should be done carefully.

The IDPS configuration is a phase that involves the configuration of the IDPS, taking into account the advantages of the system and the type of attack to be encountered. The IDPs configuration includes rules, filters, and parameter settings that can be used to detect and prevent attacks.

At the IDPS testing stage, we used SQL injection and Syn Flood Attack attacks on the conImaged system. Tests are being carried out to ensure that the IDPS can detect and prevent the plague effectively.

IDPS Performance Assessment: The final stage involves an IDPS performance evaluation taking into account factors such as detection accuracy, response speed, detection efficiency and resource playability (RAM). IDPS' performance assessment is carried out to ensure that IDPS can operate effectively and does not negatively affect system performance.

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. X No 1, Desember 2023, hlm. 171 - 178 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v10i1.2880
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

RESULTS AND DISCUSSION

In IDPS Suricata's design to detect and mitigate open-ended SQL injection, port scanning and syn flood attacks, steps are required to get results that match the purpose of a study. In the design of a phased system, determining the specification of the software hardware is very important, as is determining how the ben-tuk topology design will be used in building a good security system. In this study, IDPS with Suricata was designed as a safe system that will protect the server from various forms of threats, such as the Suricate IDPS design for detecting and mitigating SQL injection, port Scanning and syn flood attacks. The form of the Suricatai IDPS topology design for this screening can be seen in Image 2.

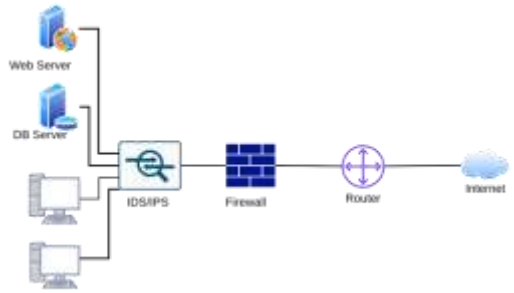

Image 2. IDPS Suricata Topology

Image 2 shows the design of the Suricata IDPS topology. Suricata locations are placed side by side with firewalls, where the two will collaborate to secure existing systems or servers. After it's done, the design of the topology is used. Then, you can implement the configuration and determine the rules used on Suricata IDPS. After all the configurations are completed, a test will be carried out by checking the configuration and the rule specified to see whether it can detect and mitigate the attack. Then, the data will be collected, which will be used to determine the form of the Suricata IDPS itself.

In testing the configuration and rule on the Suricata IDPS in this query, an SQL injection attack is carried out targeted at the server.

Image 3. SQL Injection Attack

Image 3 shows a form of SQL injection that is directed to the URL as the IP address of the server. This attack is very dangerous because it will target a database that contains information such as a system ID and password. The next attack to be tried in this study is the Syn Flood Attack, or Danial of Service. This attack will affect the source on the server, and this attack can be done with hping 3 tools, for example: hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.43.229. Then the next attack used was port scanning with NMAP, as shown in Image 4.

Image 4. *Port Scanning*

Image 4 shows the form of port scanning attacks against targer servers and will test how Suricata IDPS detects and mitigates attacks.

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. X No 1, Desember 2023, hlm. 171 - 178 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v10i1.2880
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

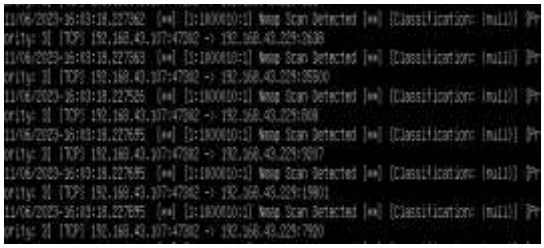

Image 5. Suricata IDPS Detection Results

Image 5 shows a successful implementation of the Suricata IDPS system. After the configuration of the Suricata is successful and running well, the data will be taken, which will be used to perform testing and analysis of the Suricata IDPS performance.

Tests are conducted using performance evaluation scenarios that include detection accuracy, detection speed, detection effectiveness and resource use. Testing activities to analyze the performance of the IDPS with the suricata are carried out every 3 minutes on each traffic that is normal traffic and traffic there are attacks. The attacks used in this test are SQL injection, syn flood Attack and port scanning. On the calculations carried out to obtain the result using the percentage of the average value.

The analytical method used to calculate the percentage accuracy is based on the accurate detection of anomalies in IDPS Suricata. The management of data obtained from IDPS can be seen in the following equation.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

Description:
TP : *True Positive*
TN : *True Negative*
FP : *False Positive*
FN : *False Negative*

The average method would work like a mathematical calculation that takes into account the amount of data. This method is used to calculate average values and test results based on detection rates. In other words, if the detection accuracy is close to 0, then the IDPS performance will be just as good. To calculate the average value, use the Berit equation.

$$\text{Average} = \sum \frac{X}{n} \quad (2)$$

Description:
X : Value of each sample.
N : The number of samples taken and used as a calculation.

Detection accuracy tests are carried out to find out from the detection results on the IDPS an indication of the existing threat. As for the accuracy of the detection, it is done under two conditions: a normal state without an attack and a state where there is an attack.

Table 1. Normal Traffic Accuracy

Activity	Suricata Accuracy
1	100%
2	98%
3	76%
4	78%
5	77%

Table 1 shows the accuracy data of the suricata in normal traffic, but the suricata detects false positives starting at activities 3, 4 and 5. The false positive itself can be understood as falsely identifying or detecting a particular event or entity as positive, whereas it should be negative. In other words, it's a mistake where the system assumes there is a problem or a threat when it actually does not exist. So-until making the accuracy change from activity 3 to 5.

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (Print)
Vol. X No 1, Desember 2023, hlm. 171 - 178 ISSN 2550-0201 (Online)
DOI: https://doi.org/10.33330/jurteksi.v10i1.2880
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

Table 2. Traffic Attack Accuracy Results

Activity	Suricata Accuracy
1	76%
2	80%
3	77%
4	86%
5	76%

In table 2, the suricata detects a true positive on the five activities carried out; in other words, it is able to detect an abnormal condition. The five activities are in the form of SQL injection, a syn flood attack, and port scanning. However, in fact, in addition to detecting true positions on the five activities, we also experienced a state of multiple false negatives or failures in detecting and dealing with the true threat of the exposure. This weakness can actually be overcome by running Suricata on a multi-core system.

At the test to see the detection speed on the Suricata against normal traffic activity and activity everywhere there are attacks.

Table 3. Suricata Speed Test Results

	Traffic Normal	Traffic Attack
Average	5,314/s	1,610/s

In Table 3, it can be seen that Suricata can be faster at detecting traffic when an attack occurs, and than testing performed, IDPS Surics can have a constant time on each detection for each attack activity performed with an average time record of 1.610/s.

In the tests carried out, the average value of the effectiveness of the Suricata IDPS was 0.242/s in normal traffic and 33.407/s in traffic under attack conditions. Suricata detection efficiency will increase as accuracy, precision, and recall increase. Accuracy measures to what extent Suricata can distinguish an attack from normal traffic; precision measures how far a positive Suri-Mata alarm really is an attack; and recall measures the extent to which Suricate can detect all attacks that are supposed to be detected.

The next test is to see the percentage of sum-ber power use by IDPS Suricata when riding under normal traffic conditions and traffic that is being attacked.

Table 4. Resource Usage

	Traffic Normal	Traffic Attack
Average	7,80%	25,84%

On table 4, you can see the average resource use on Suricata IDPS when running, where in normal traffic conditions there is an average value of 7.80% and in traffic conditions there are attacks carried out with a mean value of 25.84%. Tests were performed by performing attacks randomly with SQL injection attacks, Syn flood Attack and port scanning, for a total of 5 activities. From the results of this evaluation, it can be seen that the IDPS is not too big in terms of using existing resources. However, this will always change depending on the number of activities that take place and of course, the use of resources will also influence the accuracy, speed and effectiveness of the detection of the resources.

CONCLUSION

The IDPS Suricata can detect attack activities that target the server, such as SQL injection attacks, syn flood Attacks and port scanning. The performance testing carried out resulted in the

average accuracy value of IDPS Suricata under normal conditions in 5 activities, namely 100%, 98%, 76%, 78%, and 77%. This value was influenced by the condition of Suricata detecting false positives in activities 3 to 5. While the accuracy of suricata in IDPS suricata traffic conditions is concluded by comparing the values of normal conditions of 5.314/s and random traffic conditions of 1.610/s, the factor that determines the speed of IDPS suricata is the placement of suricata in the system, which should have multicore CPU resources. In the tests carried out, the average value of the effectiveness of IDPS Suricata was 0.242/s in normal traffic and 33.407/s in attack-condition traffic. Then the final test results are to see the amount of resource consumption by Suricata with an average value of 7.80% in normal traffic conditions and 25.84% in traffic conditions where there are attacks carried out.

BIBLIOGRAPHY

[1] D. Kurnia, "Analisis Forensik Serangan SQL Injection dan DoS Menggunakan Instrution Detection System Pada Server Berbasis Lokal," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 4, no. 2, pp. 208–212, 2020, [Online]. Available: https://jurnal.uisu.ac.id/index.php/infotekjar/article/view/2420

[2] R. A. Dalimunthe and S. Sahren, "Intrusion Detection System and Modsecurity for Handling Sql Injection Attacks," *... Soc. Sci. Inf. ...*, vol. 4509, pp. 187–194, 2020, doi: 10.33330/icossit.v1i1.711.

[3] Nursapdahi, A. Senja Fitrani, M. Alfan Rosid, and S. Aji, "Studi Analisa Serangan Sql Injection," *Semin. Nas. Inov. Teknol.*, pp. 185–190, 2022, [Online]. Available: https://proceeding.unpkediri.ac.id/index.php/inotek/article/view/2474

[4] S. Sahren, "IMPLEMENTASI TEKNOLOGI FIREWALL SEBAGAI KEAMANAN SERVER DARI SYN FLOOD ATTACK," *JURTEKSI (Jurnal Teknol. dan Sist. Informasi)*, vol. 7, no. 2, pp. 159–164, Apr. 2021, doi: 10.33330/jurteksi.v7i2.933.

[5] G. K. S. A. Putra, F. Indrajid, K. F. Andika, K. K. Bramanda, I. G. A. J. Saskara, and I. M. E. Listartha, "Analisis Hasil DoS SYN Flood Attack Pada Web Server," *Format J. Ilm. Tek. Inform.*, vol. 12, no. 1, p. 1, 2023, doi: 10.22441/format.2023.v12.i1.001.

[6] E. H. Kalabo, "Analisa Performa Intrusion Detection System (IDS) Snort Dan Suricata Terhadap Serangan TCP SYN Flood," *J. Repos.*, vol. 4, no. 3, pp. 397–406, 2022, doi: 10.22219/repositor.v4i3.1407.

[7] Prendi Parluhutan Simandalahi, "Analisis Serangan SQL Injection Pada Web Server Menggunakan Intrusion Detection System".

[8] E. Stephani, Fitri Nova, and Ervan Asri, "Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server," *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 1, no. 2, pp. 67–74, 2020, doi: 10.30630/jitsi.1.2.10.

[9] M. A. Saputra, H. H. Kusuma, and A. Ibrahim, "Mengatasi Keamanan di dalam SQL Injection dan Cara Pencegahannya," *Pros. Annu. Res. Semin. 2017 Comput. Sci. ICT*

ISBN, vol. 3, no. 1, pp. 105–108, 2017.

[10] N. L. Putri, R. A. Nugroho, R. Herteno, and P. Korespondensi, "INTRUSION DETECTION SYSTEM BERBASIS SELEKSI FITUR DENGAN KOMBINASI FILTER INFORMATION GAIN RATIO DAN CORRELATION INTRUSION DETECTION SYSTEM BASED ON FEATURE SELECTION WITH FILTER COMBINATION OF INFORMATION GAIN RATIO AND CORRELATION," vol. 8, no. 3, pp. 457–464, 2021, doi: 10.25126/jtiik.202183154.

[11] F. Raditya and J. Sidabutar, "JEPIN (Jurnal Edukasi dan Penelitian Informatika) Analisis Rules Intrusion Detection Prevention System (IDPS) Suricata untuk Mendeteksi dan Menangkal Aktivitas Crypto Mining pada Jaringan".

[12] D. T. Yuwono, "Analysis Performance Intrusion Detection System in Detecting Cyber-Attack on Apache Web Server," *IT J. Res. Dev.*, pp. 169–178, Feb. 2022, doi: 10.25299/itjrd.2022.7853.