Measuring Detection of Signature On Enterprise Computer Network

IOP Conf. Series: Materials Science and Engineering **662** (2019) 052008 doi:10.1088/1757-899X/662/5/052008

Measuring Detection of Signature On Enterprise Computer Network

S Alviana[1], I D Sumitra[2]

[1]Departemen of Informatic Engineering, Universitas Komputer Indonesia, Indonesia
[2]Departemen of Postgraduate of Information System, Universitas Komputer Indonesia, Indonesia

Email: sopian.alviana@email.unikom.ac.id

Abstract. The purpose of this study is to measure the comparative success rate methods of signature-based anomaly based on enterprise computer network attack detected. The application of information technology in many fields often cause the occurrence of attacks and threats that lead to data loss, the crippled system, and destruction of the system. To address these threats required the presence of early detection against any threats that occur at the enterprise computer network system. Early detection function to minimize and prevent the loss of the more extensive system. Methods used in the detection of the threat that is signature based and anomaly-based method. Both methods are used for detection of any threats to the network system, then that method will be between the two measured how many threats can be detected by both methods, and measure the level of success detection. The results obtained in this study, Method of Anomaly Based successfully detect 89.66% attack, while the method Signature based successfully detected 91.87% attack. If the results of the great early attack detection, then the security level of the network are also great and can reduce the risk posed by a threat.

1. Introduction

The technological advancement in computer network system and its related infrastructure is the reason for an increased occurrence rate of computer intrusions. An intrusion is defined as any set of actions to violate the security protocol of a computer network system [1][2]. Intrusion detection is one of the activities of existing hazardous activity monitor in a computer network. Intrusion Detection System (IDS) was one of the security systems used to detect any interference or threats in a computer network. Intrusion detection system in detecting any threat using two techniques, i.e., Anomaly-based and Signature-Based Detection.

Anomaly detection is one of the techniques in intrusion detection with intrusion activity with activities to differentiate normal system [3]. Anomaly-based IDS detects abnormal behavior in computer systems and computer networks. Deviation from normal behavior is considered an attack [4]. Amaral et al develop intrusion detection for wireless network based on signatures and behavior that is not normal. intrusion detection is categorized into three modules related to supervise the traffic packet data [5]. Anomaly-based intrusion detection is one of the techniques that promise, because it allows detecting unknown attacks previously [6]. Signature-based detection approach with signature-based, find the package and compare it with a standard arrangement or pattern that has been stored in the database [4]. In detection using signature based, attacks follow patterns that are already well defined to exploit the weakness of the system. Because each attack followed a pattern that is defined, then the patterns encoded first and then used to match the right user behavior [7]. The root means square error (RMSE) has been

used as a statistical method for measuring the performance of the model of meteorology, air quality, and climate research studies [8]. RMSE is an alternative method to measure the level of accuracy of the results of the estimation of a model or experiment results, in this case, an experiment testing the success rate of the method signature and anomaly-based detection. Previous research has much to use intrusion detection as a technique to detect any threats in a computer network. IDS techniques used by using signature based and anomaly-based detection.

Shijoe jose using host intrusion detection system for detection of anomaly-based instruction. Anomaly-based can detect denial of service and inform the system administrator that is a threat [3]. Pavel nevlud using anomaly-based detection to monitor the state of a network that covers the activities different from normal operation. The result of the different operations is used for analysis using machine learning [9]. Liu Hua Yeo describes the intrusion detection system using signature and anomaly based. Both techniques have advantages and disadvantages of each so that we can determine the proper techniques in each different situation [10].

Thus, this research aims to measure the success rate of some detection method using IDS signatures or anomaly based in detecting any threats which occurred in a computer network.

2. Research Methodology

Stages of research methodology include the design of a system intrusion detection system that will be used. The system is built is a network-based IDS system as shown in Figure 1.

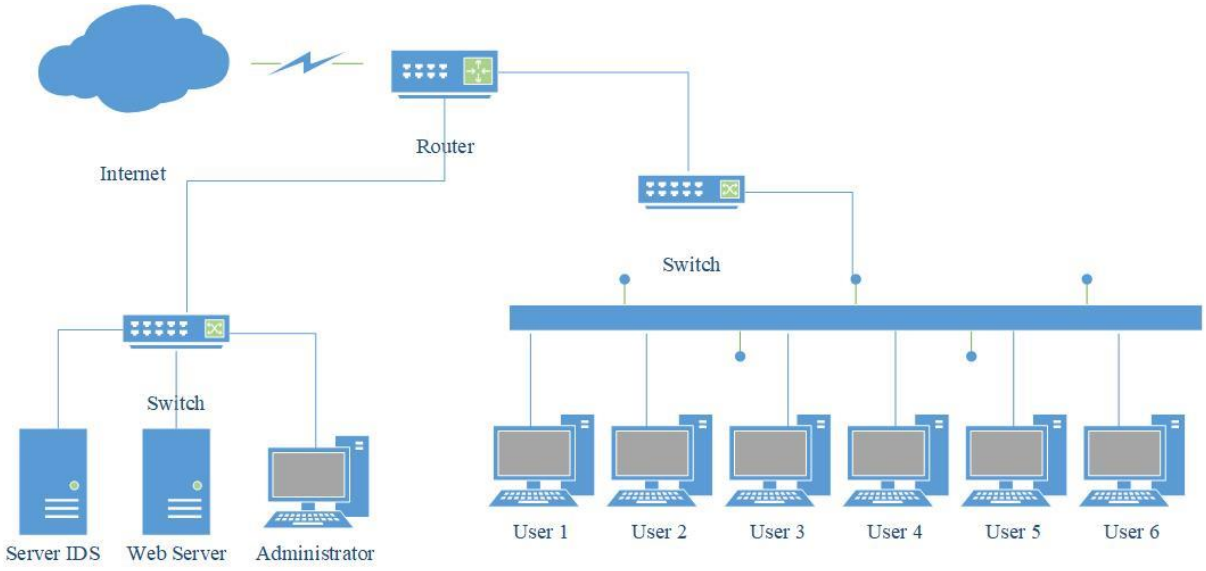

Figure 1. The Intrusion detection design system

Figure 1 describes the design of the system used to test the success rate of the detection method signatures or anomaly based. The web server is used as an object which is attacked by some users. Server IDS will check every data packet and traffic through any network, in case of the existence of activities which are regarded as a threat, administrators will find information about the occurrence of threats as early detection and can take action early to avoid the threat continues. Testing the detection success of each method is tested with a few circumstances and threats. Include UDP flood, ICMP flood, Smurf attack, Syn attack, Fin attack, and malware in the form of Trojan.

The web server will load given the threat by the type of threat that is used. Later, the IDS will be installed interchangeably with either signature or anomaly based. Each method that is applied will be measured the success rate of any detection methods. Results of detection of each method, then the

method will use the root mean square error (RMSE) to computes the percentage success rate of detection of any given threat against the method.

3. Results and Discussion

In the process of testing, each method used some attacks with the rise in the value of threat in multiples of two thousand threats. The threat of testing done within fifteen minutes, to get the number of attacks detected by any method. Following the results of detection of the number of attacks, each method IDS are used as indicated by Table 1.

Table 1. Results of detection threats

The number of threats (in thousands)	This type of threat	The number of threats detected (in thousands)		
		Without IDS Method	Anomaly-Based	Signature-Based
2		0	0,765	1,204
4		0	1,367	2,556
6		0	1,854	3,024
8	UDP Flood,	0	2,469	3,345
10	ICMP Flood,	0	2,481	3,818
12	Smurf attack,	0	2,447	4,302
14	Syn attack, Fin	0	2,400	4,821
16	attack, and	0	2,433	5,414
18	Malware	0	2,402	5,840
20		0	2,493	6,329

Table 1 shows the result of some threats detected every method. The threat is done starting with the amount of 2000 and offered up with intervals of two thousand to the value of 20.000 threats. An investigation by the table can be seen in a comparison of the number of detection that is produced by both methods. For ease in reading the results of each method to detection intrusion detection system, then the graph is shown in the comparison the amount of threat detection by signature-based and anomaly-based towards the amount of a given threat as shown in Figure 2.

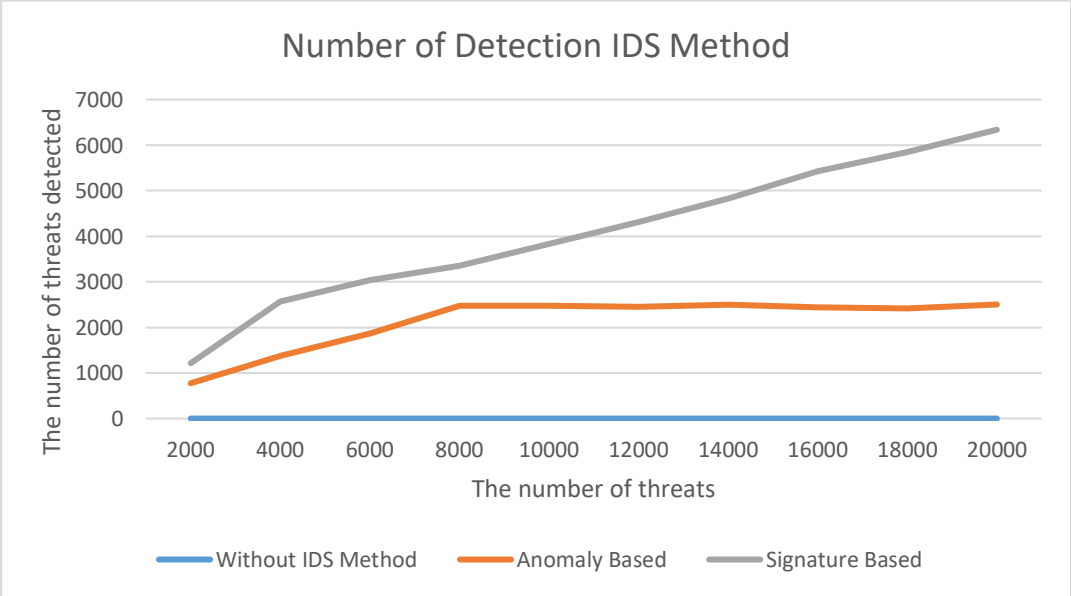

Figure 2. Graph the number of threat detection

From Figure 2, the number of detection methods comparison of visible signature and anomaly based. The interval the number of attacks that offered up the continuously apparent success of the detection method of signature-based detection has more than a method of anomaly based.
To analyze the error level generated by any method of intrusion detection systems good signature-based or anomaly based used calculations use the root mean square error (RMSE). From a large number of experiments, the calculated value of error detection is generated by each method.
The results of the calculation of the value of the error using the RMSE method are (Table):

Table 2. Comparison of values of RMSE

Value of RMSE		
Without IDS Method	Anomaly-Based	Signature-Based
12,4	10,34	8,13

Table 2 shows the results of the analysis of the level of error by using the root mean square error. The results indicate that the method of anomaly-based has value RMSE 10.34, while the method signature based has value RMSE 8.13. From the results of the calculation of the error rates can be described as a comparison of the value of the error and the success rate of the two methods of intrusion detection system as shown in Figure 3.

Figure 3. Comparison of the results of detection and error detection

Comparison of the results of detection and error detection that is generated by using the RMSE as in Figure 3 it brings results, namely:

1. Normally network traffic without IDS method has a success rate 87.6% detection and error detection rate of 12.4%.
2. The method of anomaly-based has a success rate of 89.66% detection and error detection rate of 10.34%.
3. The method of signature-based has a success rate of 91.87% detection and error detection rate of 8.13%.

Comparison of the detection and error detection showed a success rate in detecting methods of attack that occurred on the network computer. RMSE value that indicates that the method is small has a smaller error rates compared to other methods. RMSE is useful to know the level of errors a method in detecting the attack happened [6]. The higher the level of detection attack is, the more reliable methods of intrusion detection system in detecting attacks. This line as mentioned by the Shah, that a good detection system is a system that can provide a higher alert [1].

4. Conclusion

The signature-based method has a better success rate in detecting threats compared with methods anomaly based or with normal traffic without IDS method, evidenced by the number of threat detection. In addition, with the percentage of the success rate of the larger signature-based methods has error detection that is smaller than the anomaly-based methods or without IDS method.

Acknowledgments

We acknowledged Directorate Application Development Training and Service Center and Informatic Engineering to place the work of research and the Division of Information Technology Infrastructure UNIKOM for data availability.

References

[1] Shah, V., Aggarwal, A. K., & Chaubey, N. (2017). Performance improvement of intrusion detection with fusion of multiple sensors. Complex & Intelligent Systems, 3(1), 33-39.
[2] McHugh, J., Christie, A., & Allen, J. (2000). Defending yourself: The role of intrusion detection systems. IEEE software, 17(5), 42-51.
[3] Jose, S., Malathi, D., Reddy, B., & Jayaseeli, D. (2018, April). A Survey on Anomaly Based Host Intrusion Detection System. In Journal of Physics: Conference Series (Vol. 1000, No. 1, p. 012049).
[4] Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1), 16-24.
[5] Amaral, J. P., Oliveira, L. M., Rodrigues, J. J., Han, G., & Shu, L. (2014, June). Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks. pp. 1796-1801
[6] Nascimento, G., & Correia, M. (2011, June). Anomaly-based intrusion detection in software as a service. pp. 19-24
[7] Kumar, V., & Sangwan, O. P. (2012). Signature based intrusion detection system using SNORT. International Journal of Computer Applications & Information Technology, 1(3), 35-41.
[8] Chai, T., & Draxler, R. R. (2014). Root mean square error (RMSE) or mean absolute error (MAE)?–Arguments against avoiding RMSE in the literature. Geoscientific model development, **7**(3), 1247-1250.
[9] Nevlud, P., Bures, M., Kapicak, L., & Zdralek, J. (2013). Anomaly-based network intrusion detection methods. Advances in Electrical and Electronic Engineering, 11(6), 468-474.
[10]. Yeo, L. H., Che, X., & Lakkaraju, S. (2017). Modern Intrusion Detection Systems. arXiv preprint arXiv:1708.07174.