International Journal of Information System & Technology
Akreditasi No. 158/E/KPT/2021 | Vol. 7, No. 2, (2023), pp. 144-150

Design and Implementation of Sucirata-Based Instrusion Detection System as a Network Security System Cloud Computers

Ali Idrus[1], Lipur Sugiyanta[2], Murien Nugraheni[3], Subhiyanto[4]*
[1,2,3] Information Systems and Technology, Universitas Negeri Jakarta, Indonesia
[4]Informatics Engineering, STMIK Antar Bangsa
Email: aliidrus@unj.ac.id

Abstract

Cloud computing is currently being developed and widely used by companies that require large and efficient computing resources. As technology evolves, security threats in cloud services continue to increase. Various threats in cloud computing technology can be avoided by maximizing the identification of security holes. Information threats associated with cloud computing require network and service security against possible attacks. Suricata is a threat detection identifier supported by existing rules. When an attack is detected, Suricata will create a log of the attack committed, Suricata can also perform automatic detection at level 7. The author collected the results of the attack in a log. Sign Suricata and the authors also evaluate whether Suricata can detect port scanning, brute force, denial of service, and backdoors for Cloud Computing. From the test results, optimal results were obtained from the results of attacks detected by the Suricata Intrusion Detection System (IDS) logs in the /var/log/suricata/fast directory.log, the author added that the Suricata configuration is not only for detection, so it can also run drops if there is suspicious activity using network filters that already exist in Suricata and manipulated configuration assumptions to optimally improve security in the cloud.

Keywords: *Intrusion Detection System, Suricata, Cloud Computing*

1. Introduction

Cloud Computing (cloud computing) is one of the technologies that is currently widely developed and used by companies that require large and efficient computing resources. Along with the development of these technologies, security threats to Cloud Computing services are increasing. Attacks that occur in Cloud Computing can cause damage and even data loss and hardware damage. Information threats in Cloud Computing demand the security of networks and services from possible attacks. Various attacks or intrusions can occur such as Denial Of Service, Port Scanning, Brute Force, and Backdoor. These attacks can aim to access application systems or try to break into networks with special access rights to access resources or services provided either in the system or network. Suricata is an IDS that can detect attack threat activities on the network assisted by existing rules. The way Suricata works is that when there is an attack, Suricata will check the existing packages / attacks through the rules made [1]. When an attack is detected, Suricata will create a log of attacks carried out, Suricata can also perform automatic detection at layer 7, namely applications such as dns, http, imap, ftp, and smtp. So that Suricata can provide solutions to improve security in Cloud Computing.

2. Research Methodology

2.1. Cloud computing

Cloud computing is a computing technology where all computer resources and resources be it memory, applications, processors, networks, and operating systems are used virtually with remote access patterns so that they can access these services anytime, anywhere as long as they are connected to the internet network [2]. services that can be chosen from Cloud Computing, namely [3]:

ISSN : 2580-7250

a) Infrastucture as a Service (IaaS)
This service is provided by providing components in the form of servers, hardware, and networks needed at a certain price. Cloud computing users can install applications used on the infrastructure.
b) Platform as a Service (PaaS)
Services that provide software systems and supporting software needed to build applications that will be installed on the server according to the needs of the organization or agency. The organization or agency then builds the required application on this platform and uses it.
c) Software as a Service (SaaS)
Services provided by providing software and applications that can be accessed by customers via the internet. Cloud computing service providers interact with users and customers through a front-end panel.

2.2. Suricata

Suricata is an IDS that is able to detect a network activity and identify attack threats assisted by integrated rules [4].

2.3. Intrusion Detection System (IDS)

Intrusion detection system is a system that can detect suspicious activity in a system or network. If suspicious activities related to network traffic are found, IDS will warn the system or network administrator [5].

2.4. Stages of Action Research

Action research as a research method, is founded on the assumption that theory and practice can be closely integrated with learning from the results of planned interventions after detailed diagnosis of the context of the problem [6]. You can see the stages of the Action Research Method in Figure 1.

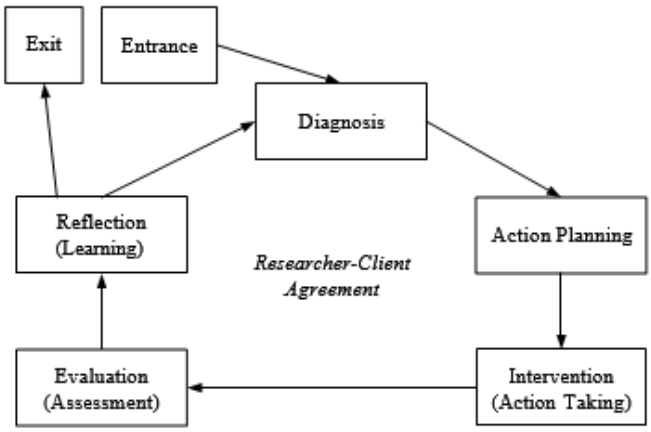

Figure 1. Stages of Action Research

Description of the stages of the method above are:

2.4.1. Diagnosis

At this stage the author identifies problems regarding cloud computing attacks such as port scanning, brute force, denial of service, and backdoor can be seen in Figure 2 [7].

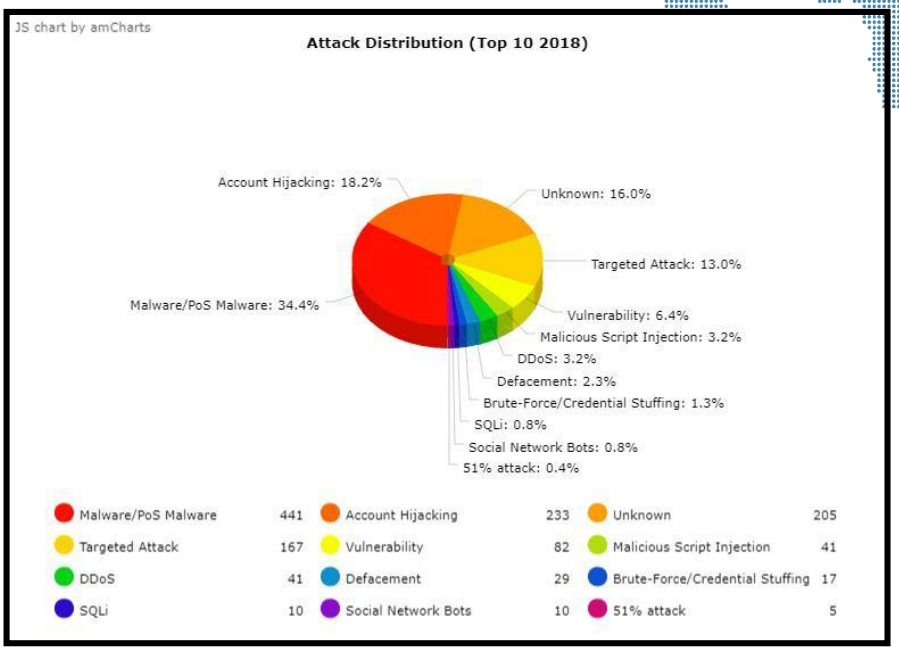

Figure 2. Cloud Computing Attacks (Hackmageddon)

The explanation from the picture above is that the author gets data on various attacks on cloud computing. The author himself obtained attack data to be tested in this study, namely port scanning entry in the Vulnerability section 6.4%, Brute-Force / Credential Stuffing: 1.3%, Denial Of Service: 3.2%, and Backdoor entry in the Malware / PoS Malware section of: 34.4%. 2.

2.4.2. Action Planning

At this stage the author understands what tools are needed, namely:

a) Virtual Private Server (VPS) which functions as a virtual server that will be installed Sulica Intrusion Detection System (IDS) software, this server will also be the target of 4 attacks from the tools provided. The author chose Digital Ocean Virtual Private Server (VPS) for 20$ / month located in Singapore and the specifications of the Virtual Private Server (VPS) Processor Intel Xeon Gold 6140 CPU @ 2.30GHz, Memory 4gb, and solid state disk (SSD), this server also has Linux operating system Ubuntu 16.04.

b) The author's attack tools also add 4 attack tools that will be used to target Virtual Private Server (VPS) that has been installed suricata. The tools of the attack are:
   1) Nmap software that functions as port scanning attack software that focuses on finding open ports on a server.
   2) Hydra software that functions as Brute Force attack software will perform forced logins periodically from the word list of passwords that have been provided by the attacker.
   3) Denial Of Service Ha3MrX software functions as attack software, the way the attack software works will send excessive packets to a server which will cause the server to go down or offline.
   4) Rootkit-Ninja software functions as a backdoor if an attacker gains user access this backdoor software will change that user's access to root access, by recalling the rootkit will turn the ordinary user into the root user.

c) Laptop Attacker author also added a laptop device to attack. The laptop uses a Linux operating system, namely Parrot OS which will use the tools provided.

d) Suricata software functions as an Intrusion Detection System that will detect what attacks will come to the Virtual Private Server (VPS) that has been provided by the author.
e) Suricata file rules function as suricata rules to be installed in the Intrusion Detection System software suricata file rules function according to what rules will be installed to detect attacks on the Virtual Private Server (VPS).

2.4.3. Intervention (Action Taking)

This stage also researchers begin to carry out attacks using tools that have been prepared and conFigure the Suricata IDS that has been prepared after completion the tester will write how the Suricata System works to detect port scanning, brute force, denial of service, and backdoor attacks in Cloud Computing.

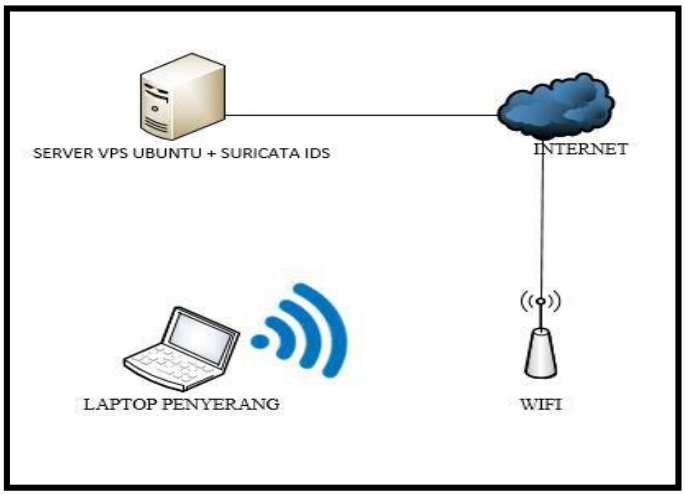

Figure 3. Attack Flow Topology

In Figure 3, this attack flow topology describes the server with the attacker's PC being on a different internet gateway. Because the server uses a rented Ubuntu Virtual Private Server while the attacker's PC is located in a different place from the server, the attacker's PC is connected to a wireless network.

2.4.4. Evaluation (Assessment)

This part of the stage the author collects the results of the attack in Suricata's logs and the author also evaluates whether Suricata can detect port scanning, brute force, denial of service, and backdoor attacks to Cloud Computing.

2.4.5. Reflection (Learning)

At this stage, the author makes a report with the results that have been obtained after conducting research.

3. Result and Discussion

The author gets optimal results from the results of the attack log detected by the Suricata intrusion detection system (IDS) which is in dir /var/log/suricata/fast.log, and also the Suricata rules are not only focused on one attack but where the attack resembles another attack it will be equally detected by the suricata. The log file also describes the time of the attack, the date, the clock, and the description of the attack. The author also added a fileswatcher to send notifications when there is a regex entered in the suricata log file which will be sent to telegram if there is an attack.

Figure 4. Telegram notifications of bruteforce attacks

The author gets the notification results from the LaporGan bot that has been created by the author to get notifications when there is an attack that enters the suricata log, namely fast.log, The type of notification is also written differently for each attack carried out by the author as Figure 4.

Table 1. Log results and impact

Attack	Log Results	Impact
Scanning Port	In *port scanning attacks* Obtained in the form of logs, namely: 02/02/2019-06:38:55.100162 [Drop] [**] [1:2018489:3] ET *SCAN NMAP OS Detection Probe [**] [Classification: Attempted Information Leak]*	Impact from attack aforementioned. Attackers can See what *service port* it is opened by the *server* And attackers can also focus attack to *Port* certain.
	[Priority: 2] {UDP} *101.128.76.135*	
Brute Force	In *Brute force attacks* Obtained in the form of *logs* , namely: *ET SCAN SSH BruteForce Tool with fake PUTTY version [**] [Classification: Detection of a Network Scan] [Priority*: 3] {TCP} 218.92.1.158:58138 -> 159.65.12.147:22	Brute force *attacks* can Cause *Usage memory* becomes high and also when *our* password Go to *Word List* Assailant so Assailant will Get *Password* to *SSH login*.
Denial Of Service	Deep attack *Denial Of Service* is obtained in the form of *logs* that is : *SERIALIZINGME SCAN LibSSH Based SSH Connections Not Allowed [**]*	Attack ini also can Cause *Server* being *down* and not can go well.
	[Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 104.131.226.221:49559 -> 159.65.12.147:22.	
Backdoor	In *Backdoor attack*	Obtained in the form of *logs* , namely: 01/17/2019-20:00:53.087437

Attack	Log Results	Impact
		[**] [1:2019876:4] *ET SCAN SSH BruteForce Tool with fake PUTTY version [**] [Classification: Detection of a Network Scan] [Priority*: 3] {TCP} 218.92.1.158:13230 -> 159.65.12.147:22

In Figure 5 the author made a bar graph, namely the percentage of attack protection 90% Scanning Port can be detected and dropped by Suricata, the percentage of attack protection 90% can be detected and dropped by Suricata, the percentage of attack protection from Denial Of Service is 90% can be detected by Suricata and 15% can be dropped by Suricata, And backdoor attacks the percentage of attack protection is 70% can be detected by Suricata and 15% can be dropped by Suricata.

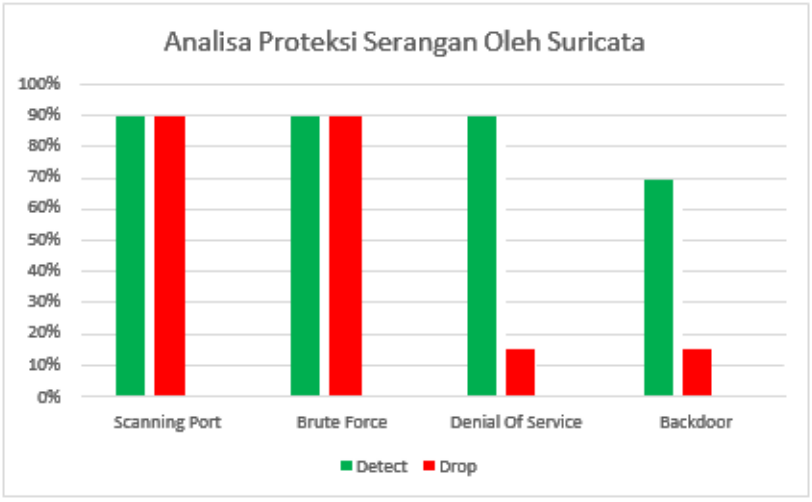

Figure 5. Suciata Protection Analysis

4. Conclusion

From these results the test gets optimal results from the results of attacks detected by Suricata's intrusion detection system (IDS) logs in dir /var/log/suricata/fast.log, and also the author adds the suricata configuration not only to detect, so it can also perform drop execution if there is suspicious activity by using netfilters that already exist in suricata and configuration by the author to increase security in cloud computing optimally. Obtained protection results from sucirata amounted to a percentage of attack protection 90% Scanning Port can be detected and dropped by Suricata, Percentage of attack protection 90% can be detected and dropped by Suricata, Percentage of attack protection from Denial Of Service is 90% can be detected by Suricata and 15% can be dropped by Suricata, And backdoor attacks 70% attack protection percentage can be detected by Suricata and 15% can be dropped by Suricata.

References

[1] Ariyanto, Yuri. Harijanto, Budi. Watequlis S, Yan. (2017). "Suricata Implementation on Proxmox VE Cloud Server as an Intrusion Detection System (IDS) in Network Security". Proceedings of Sentrinov, p TE178-TE179.

[2] Athailah. (2013). "A Quick Guide to Mastering the Router." Jakarta: PT. TransMedia, p. 6-15.

[3] Atmojo, Y. P. (2018). "Snort Bot Alert with Telegram Bot API on Intrusion Detection System." IDS Case Study on Web Server, 176–180.
[4] Badrul, M. (2012). "Network Computer Engineering." East Jakarta: Inti Prima Promosindo, p. 64-66.
[5] Eka P, Ricky. Rachman, Andy. and Wahyu H, Tri, (2010). "Virtual Private Server (VPS) as an Alternative to Dedicated Server." Surabaya: Sepuluh Nopember Institute of Technology, 2010.
[6] Fajrin, T. (2012). "Analysis of data storage systems using systems. Cloud Computing Case Study of SMK N 2 Karanganyar." 1 (10), p. 31– 35.
[7] Gaddafi, S., Meilani, D. B., and Arifin, S. (2017). "Open Cloud Computing Security System Using IDS (Intrusion Detection System) and IPS (Intrusion Prevention System)". Journal of Science and Technology, 21(2), p. 67–76.

Authors

Ali Idrus, *Information Systems and Technology Study Program, Faculty of Engineering – Jakarta State University*

Lipur Sugiyanta, *Information Systems and Technology Study Program, Faculty of Engineering – Jakarta State University*

Murien Nugraheni, *Information Systems and Technology Study Program, Faculty of Engineering – Jakarta State University*

Subhiyanto, *Informatics Engineering Study Program, STMIK Antar Bangsa*