2020 Information Technology International Seminar (ITIS)
Surabaya, Indonesia, October 14-16, 2020

Network Security System on Multiple Servers Against Brute Force Attacks

Mohammad Idhom
Departement of Computer Science
UPN "Veteran" Jawa Timur
Surabaya, Indonesia
idhom@upnjatim.ac.id

Henni Endah Wahanani
Departement of Computer Science
UPN "Veteran" Jawa Timur
Surabaya, Indonesia
henniendah.if@upnjatim.ac.id

Akhmad Fauzi
Departement of Computer Science
UPN "Veteran" Jawa Timur
Surabaya, Indonesia
akhmadfauzi@upnjatim.ac.id

2020 6th Information Technology International Seminar (ITIS) | 978-1-7281-7726-7/20/$31.00 ©2020 IEEE | DOI: 10.1109/ITIS50118.2020.9321108

***Abstract*— Network security is critical to be able to maintain the information, especially on servers that store a lot of information; several types of attacks can occur on servers, including brute force and DDoS attacks; in the case study in this research, there are four servers used so that a network security system that can synchronize with each other so that when one server detects an attack, another server can take precautions before the same attack occurs on another server.fail2ban is a network security tool that uses the IDPS (Intrusion Detection and Prevention System) method which is an extension of the IDS (Intrusion Detection System) combined with IP tables so that it can detect and prevent suspicious activities on a network, fail2ban automatically default can only run on one server without being able to synchronize on other servers. With a network security system that can run on multiple servers, the attack prevention process can be done faster because when one server detects an attack, another server will take precautions by retrieving the information that has entered the collector database synchronizing all servers other servers can prevent attacks before an attack occurs on that server.**

***Keywords*— Network security, Fail2ban, IDS, IDPs**

I. INTRODUCTION

At this time, many network security systems on servers cannot analyze and make decisions when an attack occurs; the network system also cannot share information on attacks that have occurred to other servers; network security systems on servers like this will be hazardous because of the attacks that occur previously it could happen again on other servers, besides that the server monitoring process will be more time consuming because you have to do monitoring alternately on each server [1].

Network security is critical to maintaining the information, especially on servers that store a lot of information; several types of attacks can occur on servers, including brute force and DDoS attacks Distributed Denial of Service (DDoS). The way these brute force attack works is to look for a valid password cracking, the brute-force attack will place or search for all possible passwords that have been provided with a certain character input and password length, this tries to combine passwords [2], while Distributed Denial of Service attacks (DDoS), this attack is used by a group of zombie computers, which means that this computer has been infiltrated by an application running in the background to send several packet data to a server, this attack is coordinated and can be carried out simultaneously without being noticed. By comp, the owner enters the zombie [3].

As reported at the end of 2014, DDoS attack is the most popular attack technique and is often used by a hacker [4]. DDoS is a major threat to cyberspace and a major cybersecurity problem. DDoS is called the weapon of choice by hackers because it has proven to be a frightening threat to users, organizations, and infrastructure on the Internet. On the other hand, a network attack is a risk for integrity, confidentiality, and availability of resources provided by the organization [5].

In another study conducted by Hendri et al [6], several approaches can be taken to address network security problems. Like using the IDS (Intrusion Detection System), IPS (Intrusion Prevention System), and IDPS (Intrusion Detection and Prevention System), IDPS itself is a development of IDS combined with a firewall, in this case, using IP Tables.

IDPs can detect intruders or malicious packages on the network and provide reports in the form of logs about network activity and conditions as well as drop packets against intrusion attempts and can be used to assist administrators in monitoring and analyzing malicious packages contained in a network [7].

Previous research on sending information on fail2ban attacks and adaptive systems on servers [8] has described the concept of a network security system on a server that can be connected to an adaptive system between servers that can share information about attacks that have occurred before. Meanwhile, research related to web server security [9] shows that fail2ban can prevent brute force attacks on the server by configuring rules on fail2ban to read attacks on HTTP / HTTPS ports. In another study, fail2ban was applied, which is used as an effort to reduce the possibility of DDoS attacks on the webserver; fail2ban is set with a maximum attempt to enter once where a failure occurs when trying to log in, blocking will be carried out immediately, and the ports that are secured are HTTP and HTTPS ports according to the type of server to be secured [10]. Furthermore, real-time notification on the server shows that fail2ban can be customized to send attack information to the database [11]. The server's monitoring system explains that a script can run at a specified time by creating a cronjob on the server so that the script can run periodically [12].

Based on previous research that has been explained, no one has researched the intrusion detection and prevention system (IDPS) on multiple servers where the system can detect and prevent attacks by blocking IP addresses

978-1-7281-7726-7/20/$31.00 ©2020 IEEE

suspected of being an attacker able to send report results automatically. Real-time using the PHP programming language where data is taken from the results of the attack log on each server, then forwarded to the collector database, the results of reports, and website-based monitoring so that the administrator can easily read the resulting output.

II. METHOD

Fail2ban is a tool that applies the IDPS (Intrusion Detection & Prevention System) method, IDPS itself is a development of IDS (Intrusion Detection System) [9] which is combined with a firewall [10]; by default, fail2ban can only be used on one server and cannot be used with each other. Connect on another server. Fail2ban runs in the background by taking over the IP tables configuration and can be easily adjusted to the needs of the system to be created; configuration of fail2ban rules can be done in /etc/file2ban/jail.conf, starting from setting the port to be secured, the filtration used for reading attacks, up to the length of time the blocking of the attacks occurred.

This journal will explain how the server process can send attack information to the collector database. Other servers can take advantage of this information to prevent attacks and explain how they can display attacks on all servers.

The author uses the design stage to create a description of the system to be built, including the topology used, the system flow, the process of sending attack information, and retrieving attack information on the collector database.

In this study, a star topology is used. This type of network topology uses one terminal as a central terminal that connects to all terminals.

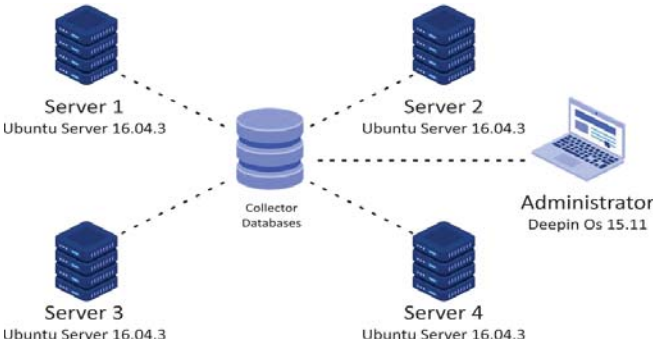

Fig 1. Topology

Fig 1. is a topological design used in this research. Four servers will be secured with a network security system that can be integrated to minimize an attack on the server.

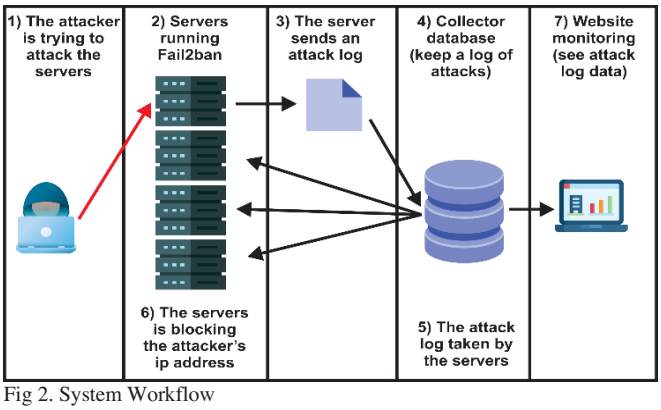

Fig 2. System Workflow

1. The attacker tries to perform a brute force attack on one of the servers running the fail2ban service.
2. The server running the fail2ban service will monitor the activity and block the attacker's IP address because it has been identified as an attacker.
3. Attack information that has been read by the server will be sent to the collector database.
4. The collector database will store all attacks that have occurred on all servers.
5. Attack information that has been stored in the collector database will be taken by another server and used as a reference for taking action.
6. The server will block the attacker's IP address based on the collector database's attack information.
7. An administrator can monitor attacks on the server in real-time on the website used as monitoring.

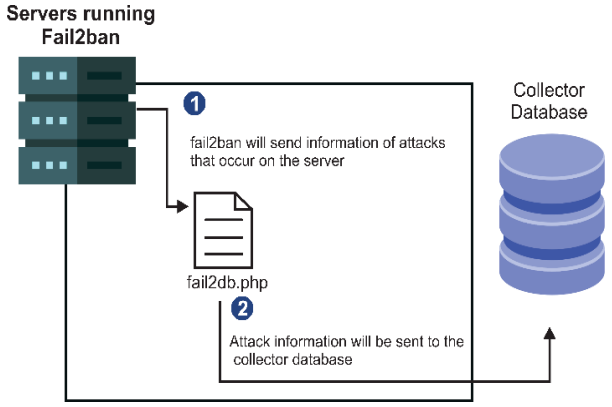

Fig 3. Information Delivery Flow

The sending attack information will be carried out when the server running the fail2ban service detects an attack. The attack information will be forwarded to the fail2db.php file and then forwarded to the collector database.

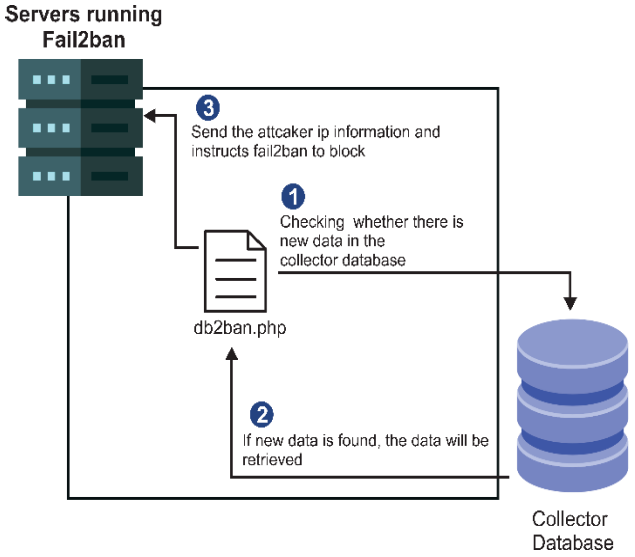

Fig 4. Flow of Retrieving Information From The Database

The process of retrieving attack information from the database is carried out by the db2ban.php file, which has been scheduled periodically [11] at cronjob so that it can check the database collector; if new data is found, the collector database, the attack information will be forwarded by the server so that fail2ban will block the attacker's internet protocol.

III. RESULTS

The implementation is based on the design and literature study that has been done.

A. *Install and configuration fail2ban*

ConFig ssh on fail2ban with the command sudo nano /etc/fail2ban/jail.local

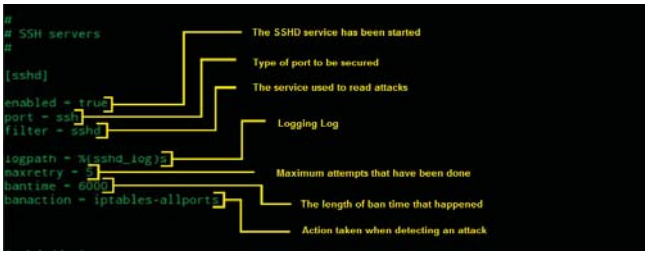

Fig. 5 ConFig fail2ban rules

This rule is applied to the ssh port; the following is an explanation of this rule.

1. "[sshd]" Is a configuration on ssh against brute force attacks
2. "[sshd-ddos]" Is a configuration on ssh against DDoS attacks
3. "enabled" Is a condition for an active rule or not
4. "port" Is a type of port that is secured
5. "filter" Is a filter that is done on the port
6. "maxretry" Is the maximum number of requests that can be done
7. "action ban" Is an action taken when an attack occurs
8. "bantime" Represents the length of time the ban will occur

Configuration banaction Banaction configuration is done so that attacks that occur can be sent to fail2db.php, the configuration is done with the command sudo nano /usr/local/fail2db/iptables.conf

Fig 6. ConFig banaction

In Fig 6 the banaction configuration on fail2ban where the configuration on banaction will call the files in the / usr / local / fail2db / fail2db directory where the files in that directory, the banaction configuration is important so that the attack logs can be sent to the database in real-time.

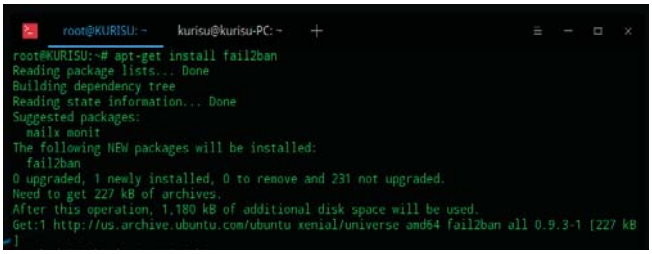

Fig 7. Result of fail2ban installation

B. *Configuration Cronjob*

The cronjob configuration is done so that the fail2db.php file can run periodically by writing the command sudo nano /etc/crontab

Fig. 8 ConFig Cronjob

In Fig 8 is a cronjob list on the server wherein the file several files will automatically run at a certain time according to the predetermined time parameters.

Fig 9. File directory / usr / local / fail2db

In Fig 9. are all files used to be able to send attack logs to the database and ban IPs in the database with time intervals of less than 60 seconds

C. *Configuration Database*

A database is a structured collection of information [12]; in this study, the database is used as a storage area for attack information and user information to enter the monitoring website.

Before testing the attack, conFig the IP address of the server, which is used as follows.

TABEL I. TESTING ATTACK

Computer	IP Addres
Attacker	192.168.43.82
Server 1	192.168.43.1
Server 2	192.168.43.107
Server 3	192.168.43.115
Server 4	192.168.43.77

The test attack is carried out using a brute force attack using the hydra tool.

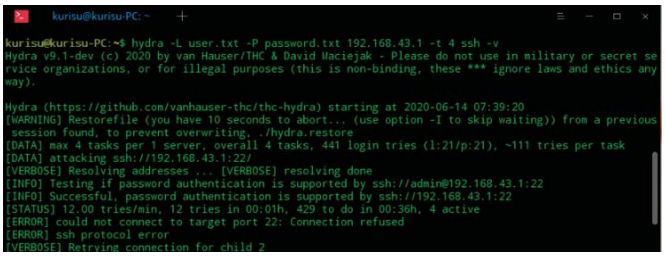

Fig 10. Attack Brute force

After the brute force attack has been carried out, then checking is carried out on the monitoring website.

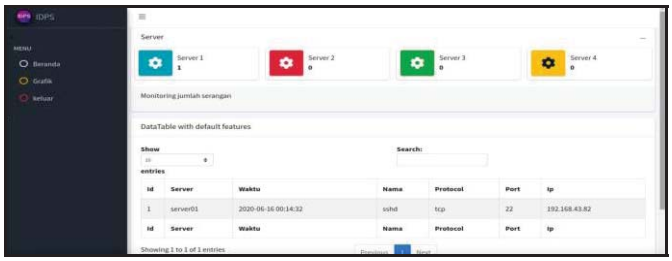

Fig 11. Website Monitoring

In Fig 9 is a display of the home page on the website, which is used as a monitoring and reporting on the security system that is made.

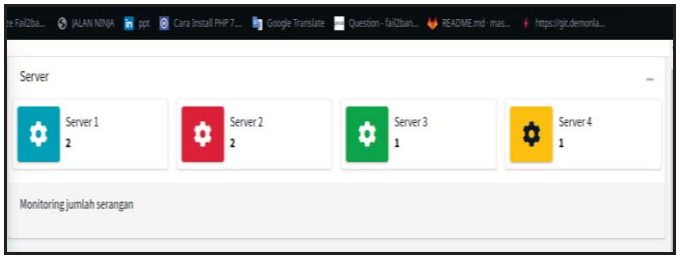

Fig 12. Widget number of attacks

In Fig 12. is a widget that displays the number of attacks on each server on the home page, data from the widget is retrieved from the database with the following script:

```
<?php
  include 'koneksi.php';
  $s1  =  mysqli_query($koneksi,  "SELECT  *  FROM  fail2ban  WHERE
  server='server01'");
  $s2  =  mysqli_query($koneksi,  "SELECT  *  FROM  fail2ban  WHERE
  server='server02'");
  $s3  =  mysqli_query($koneksi,  "SELECT  *  FROM  fail2ban  WHERE
  server='server03'");
  $s4  =  mysqli_query($koneksi,  "SELECT  *  FROM  fail2ban  WHERE
  server='server04'");
?>
```

Fig 13. Script new variables

The script is used to define new variables where these variables take data on the server's attacks, which will later be displayed on the website.

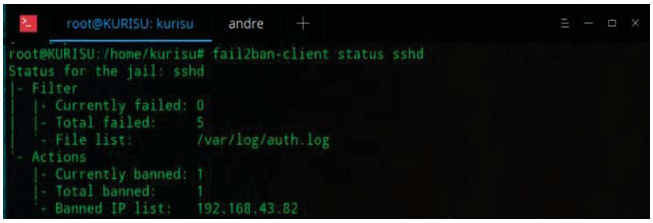

Fig 14. List ban on other servers

From the results of the testing that has been done, it is proven that the server that has been attacked can take precautions and has succeeded in sending information on the attack that occurred to the collector database. It can retrieve attack information on the collector database and then block the attacker's IP on other servers.

IV. CONCLUSION

In a network security system created by the IDPS method, the IDPS method is applied to multiple servers so that when one server detects and prevents attacks, the other server will prevent attacks by banning the IP; other servers can take precautions because when one server is attacked, then The server will send the attacker's data to the collector database so that other servers can retrieve the data to be banned. To detect and prevent brute force and DDoS attacks on the ssh port on fail2ban, configuration fail2ban rules on the server where the maxretry, bantime, fine time, and ban action rules can be adjusted to detect and prevent attacks.

In getting a ban based on existing data in the collector database, a file written in the PHP programming language is needed, where the file will read the data in the collector database so that when there is a new log in the collector database, it will be banned on IP, the file used to read the attack logs from the database collector, cannot be executed automatically when there is new data in the collector database, so a cronjob is needed so that the file can be run automatically. The network security system created in this study uses website-based monitoring which can display logs of attacks captured by each server; in addition to displaying attack counters on each server on the website, it can also display a graph of the number of attacks on each server, and attack logs on the website. It can be saved in pdf form to be used as a reference for evaluating the security system used in the future.

V. ACKNOWLEDGMENT

The author's thanks to the University of Pembangunan Nasional Veteran Jawa Timur, especially for Informatics and Computer Science Department, for providing financial support for this Research.

VI. REFERENCES

[1] [Ford, M., Mallery, C., Palmasani, F., Reid, M., Turner, R., Soles, L., and Snider, D. “A Process to Transfer Fail2ban Date to an Adaptive Enterprise Intrusion Detection and Prevention System,” IEEE, 2016.

[2] Pratita, H. S,. “Brute Force Attack Analysis Using Application Scanning on HTTP Attacker”, 2016.

[3] Airlangga, G., and Mualo, A. “Use of Brute Force Algorithm in DDOS Attack Types to Test Website Defense, ” *National Seminar on Information and Communication Technology 2015* (SENTIKA 2015), 417-423, 2015.

[4] ArborNetworks, “Worldwide Infrastructure Security Report,” ArborNetworks, 2014.

[5] Zhao, T., Lo, D. C.-T., and Qian, K, “A Neural Network-Based DDOS Detection System Using Hadoop and Hbase”. IEEE, 1326-1331, 2015.

[6] H. Alamsyah, Riska, and A. Al Akbar, “Network Security Analysis Using Network Intrusion Detection,” *Journal of Information Technology*, pp.17-24, 2018.

[7] M.S. Husain S.S, LM, Fid Aksara, and N. Ransi, “Implementation of Server Security in Wireless Networks and Prevention System (IDPS) (CASE STUDY: TECHNO'S STUDIO),” SemanTIK, pp.11-20, 2018

[8] A.S. Petrosyan and G.S. Petrosyan, "Development and Implementation of Some Advanced Web Server Protection Methods," Mathematical Problems of Computer Science, pp. 66-72, 2016.

[9] T.M Vidyapeeth, P. “Mitigation of The Risk Factor on Apache Web Server from DDoS Attacks,” IEEE, 2018.

[10] F. Arsin, M. Yamin, and L. Surimi, "Implementation Security System Using the IDPS (Intrusion Detection and Prevention System) Method With Realtime Notification Services," semanTIK, pp. 39-48, 2017.

[11] I. H. Abd Halim, N. M. I. Abu Hasan, T. R. Razak, M. N. Fikri and M. H. Ismail, "Reducing Honeypot Log Storage Capacity Consumption – Cron Job with Perl-Script Approach," Journal of Computing Research & Innovation (JCRINN) , Vols. Vol 4, No 1, pp. 16-26, 2019.

[12] Bhagya Roy and Dr. Joby P P, "Analysis and Detection of Malware Using Intrusion Detection Technique," International Journal of Applied Engineering Research, Vols. Vol 15, No 7, pp. 628-630, 2020.

[13] D. Gunawan, "Evaluation of Database Splitting Performance with Classification Methods on Data Mining Preprocessing Data," KHAZANAH INFORMATIKA Journal of Computer Science and Informatics, 2016.

[14] D. P. K. K. H. A. W. Taufan, "Network Monitoring System on Linux Server Using Sms Gateway," JMASIF, Vols. vol 2, no 3, pp. 63-72, 2011.

[15] J. Pokorny, "NoSQL databases: a step to database scalability in a web environment," International Journal of Web information systems, vol. Vol. 9 No. 1, pp. 69-82, 2013