Jurnal Komputer dan Elektro Sains, Vol.3 No.1, March 2025, 28-32
https://ejournal.sultanpublisher.com/index.php/komets

Received : 03-10, 2024, Revision: 10-10, 2024, Acepted: 12-10, 2024, Publication: 11-01, 2025.

ISSN Online 3021-8462, DOI : https://doi.org/10.58291/komets.v3i1.305

Risk Analysis of Brute-force Attacks on Webserver with Telegram Notifications

Budi Wibowo and Luqman Hafiz

Department of Informatics Engineering, Institut Teknologi Budi Utomo, Jakarta, Indonesia

Author Correspondence: (e-mail: budiwibowo1993@gmail.com)

ABSTRAK

In today's digital era, server security is a top priority for many organizations. Intrusion Detection Systems (IDS) such as Fail2ban, have proven effective in protecting servers from threats by monitoring logs and blocking suspicious IP addresses. This paper discusses the implementation of Fail2ban integrated with Telegram notifications, how it works, testing, and results showing improvements in detecting and responding to attacks. Server ssh brute force attacks pose considerable risks to web servers and have potentially severe consequences. Implementing strong preventive measures, continuous monitoring, and leveraging Telegram notifications for real-time alerts significantly improved the organization's security posture. These combined efforts ensure robust and responsive detection of brute force attacks. Fail2ban was able to quickly discover the IP address from which the attacker performed the brute force attack and took preventive action by blocking the attacker's Ip for 3 failed login attempts within a specified time limit of 3600 s.

KEYWORD Brute force attack, Intrusion Detection System (IDS), Real-time alerts, Automated threat detection

1. INTRODUCTION

The rapid development of technology with various functions and conveniences is increasing regarding its security, especially in systems that store a large amount of information. Continuing infrastructure advances and complex systems are not free from potential security vulnerabilities in terms of system configuration and functionality.[1] Widespread data leaks, especially information leakage to unauthorized parties, are very harmful to system owners and users with information data.[2) More accessible information about hacking and cracking knowledge in cyberspace makes it more accessible, and many cybercriminals perform infiltration. Or attack. Attacks are carried out massively and continuously, where the problem is challenging to monitor manually in real-time by the administrator; however, these attacks can occur at any time.[3] Attacks often occur, including a Brute force login and spontaneous activity performed automatically with tools searching for all possible valid usernames and passwords. [4] In future work, we will focus on preventing brute force attacks. The attack logs are then sent to the database. Then notifications will be sent via the Telegram platform to stop attacks and simplify the classification and analysis process, producing output that is easy for administrators to read if there is an attack on the server and administrators can overcome it against attacks on the server [5].

Arif Rahman et al. A previous study analyzed notification systems built using Snort as NIDSs with WhatsApp and Telegram as notification platforms.[6] Furthermore, Budi Wibowo et al. Research discussed smart homes with the Internet of things being attacked and then providing attack notifications via telegram. This research introduces a Telegram-based notification system to provide real-time alerts when brute force activity is detected on a web server. This method provides an advantage over traditional methods that do not provide instant notifications or use less efficient notification systems.[7] By using Telegram, the system allows administrators to respond quickly to brute force attacks. Alerts sent via Telegram can be received instantly on mobile devices, allowing for a faster response compared to other notification methods that may require logging into a security system or monitoring a dashboard [8].

Thus, from the above problems, it facilitates and performs automatic prevention and helps the work of system administrators who can be accessed remotely or systems that can detect attacks automatically, provide analysis, or report results against attacks. Therefore, this study aims to minimize the threat of attacks from internal or external parties in cyberattacks by blocking access to servers with social media telegram notifications in real-time. and ban any IP that attempts to log in too many times or performs other unwanted

actions within a timeframe set by the administrator.9] Brute force attacks involve systematically attempting numerous combinations of usernames and passwords to gain unauthorized access to a web server.[10][11] The increasing sophistication and automation of such attacks requires robust detection and response mechanisms. This study focuses on integrating Telegram notifications for real-time alerting to enhance the response to brute force attacks.[12]

2. METHOD RESEARCH

This study demonstrates that telegram-based notification systems offer advantages in terms of speed and ease of access compared to previous methods that rely on email notifications or web-based monitoring systems. Although emails may be delayed or caught in spam filters, Telegram notifications are received faster and are received immediately on mobile devices.[10] This study provides empirical data demonstrating that Telegram notification systems are more effective in improving responses to brute force attacks than other less real-time notification methods. Previous studies have described various detection methods for brute force attacks, but not many have integrated real-time notification systems, such as Telegram. This study aims to fill this gap by analyzing the effectiveness of Telegram notifications in terms of improving responses to brute force attacks.[13] The first step in this method is to identify suitable research methods, where the researcher lists and collects data from various sources to determine the prevention methods needed to prevent brute force attacks.[14] Secondly, the literature study stage is conducted, which involves collecting the theoretical basis that supports the research. The literature used includes journals, articles, and books related to brute force attacks. In the third stage, the researcher selects the method to be used.6][10][15] In this stage, the parameters to prevent brute force attacks are determined using an intrusion prevention system (IPS) that works based on predefined parameters.[11] The researcher configured the system such that if an attacker attempts to log into the SSH session three times, the system will block the IP address.[16] The next step was to build the research environment with all the software components required in this research. The final stage of the process was testing and data collection, during which the researchers tested a three-stage system. In the first stage, the target was attacked without the protection of the Fail2ban security system. In the next stage, an attack was carried out with Fail2ban enabled, which blocked the attack and displayed a log of the IPs that had been blocked.

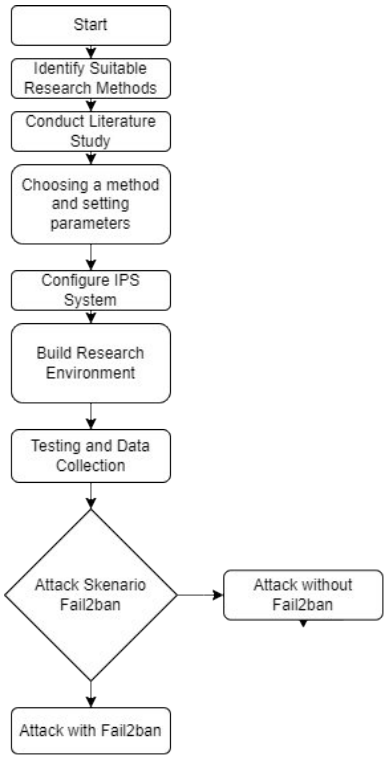

Figure 1. Represents each step in the research methodology.

The Method used in this study is a research-and-development approach [11]. In this study, the methodology used is as follows: Literature Study , At this stage, data related to the threat of brute force attacks. Stage of Analysis, At this stage, the researcher analyzed tools and work processes. Stage of the test, In this process, a brute-force attack simulation is performed against predetermined targets that Fail2ban has not yet implemented. Where Fail2ban works by automating firewall configurations on the server, and when functioning, Fail2ban takes over the firewall function on the server side.[12] Implementation and Configuration, This stage implements Fail2ban and integrates notifications via telegram as information about brute-force attacks on the server side.[13]

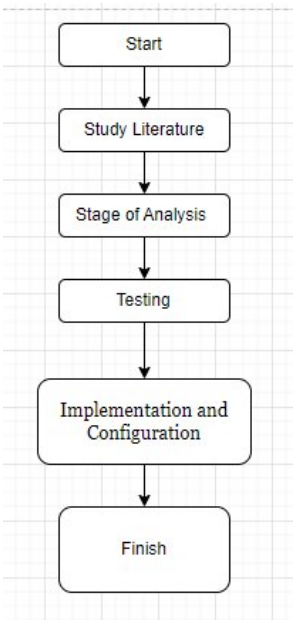

Figure 2. The following describes the process of building this system.

The ability to decompose complex problems or information into smaller, more understandable parts is referred to as analysis. In addition to the tools and equipment required for their research, researchers also use security measures, such as scanning and blocking attackers' IP addresses to protect their servers from attempts to steal or tamper with data by irresponsible parties.

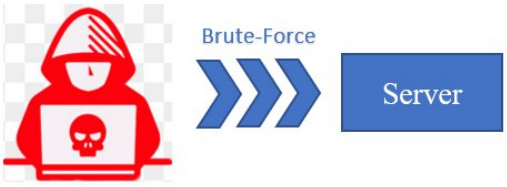

Figure 3. Attacker attempting to perform an attack

During the research process, several stages of the process are needed to build an IDS system, and the results are presented as notifications that reach the administrator through Telegram.The following describes the process of building this system (Figure 1).

3. RESULTS AND DISCUSSION

The result of this investigation describes a notification of brute force attack activity recognized successfully by the fail2ban installed server based on an agreement with the specified rules. Network security monitoring notification systems require a fast response time to allow administrators to receive notifications quickly.This is necessary so that administrators know what steps should be taken to prevent attacks . If this step is dangerous, further action is required to prevent significant damage to the server. The research process requires several stages to build an IDS system, the results of which are communicated to the administrator via Telegram .

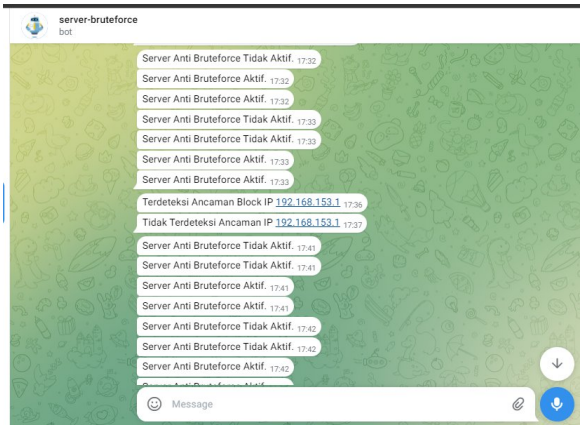

Figure 4. Brute force attack notification

Based on the test results, the Fail2ban IDS software was found to be effective in detecting attacks that enter the server, blocking the source IP of attacks, and informing administrators about attacks via the Telegram application. The following is the basic configuration of the fail2ban server design to implement preventive measures on the 192.168-shared network segment.153. x in table 1 the fail2ban configuration is complete. Here, create a copy of jail.conf cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local. by creating blocking / banned rules

Table 1. fail2ban configuration banned rules

ignoreip = 127.0.0.1/8 192.168.153.10
bantime = 3600
findtime = 120
maxretry = 3

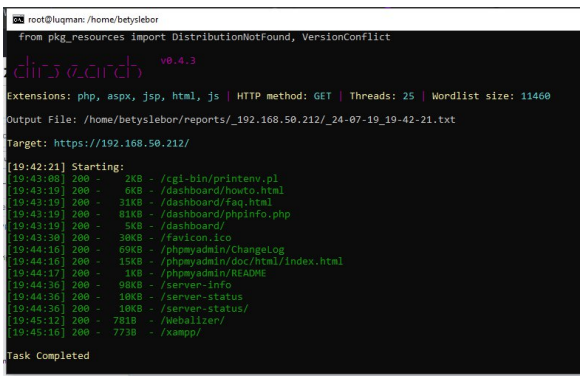

Figure 5. Directory attack on web server with 200 code response condition

From the attacker or hacker side, two directories with code 200 were detected, whose data is represented. The attack log on port 80 of the webserver from the hacker side is also included. The analysis of the Wazuh SIEM data acquisition revealed the standard deviation value of the attack. In the attack, the tools used attempted to guess the directory of the 12,361 hits detected by Wazuh. Then, a hacker experiment was conducted to perform scanning with directory search conditions with a status code of 200, which means that , the directory is valid in the webserver directory location. With payload insearch -u (target ip) -include-status=200, as shown below, the directory is displayed only with a 200-response code that will be displayed on the hacker terminal.

During testing, Fail2ban successfully detected brute force attacks against SSH services with high accuracy. The proposed tool effectively recognizes suspicious login attempt patterns and sends notifications to system administrators. Whenever a brute force attack is detected, the system automatically performs response actions according to the predefined configuration. These responses include blocking the source IP address, providing security alerts, and logging the event for further auditing. Based on the test data, it could recognize more than 95% of brute force attacks on the monitored services. This demonstrates the system's reliability and quick response rate despite evolving security threats. Replace [IP_Address_Server] with the IP address of the targeted Wazuh server.

The following commands are used to run a brute force attack:

#hydra -L username.txt -P password.txt ssh://[IP_Address_Server]

The responsiveness of the IDS system is determined by the responsiveness of the length of the system to detect attacks until the system successfully sends notifications to the administrator. The results of testing the level of responsibility were used to measure the effectiveness of the proposed IDS system and the use of Telegram as a medium for delivering intrusion notifications. The detection speed time is calculated based on the average obtained from the difference between the time the attack starts and the time the attack is detected by the IDS system. In addition, the notification speed time can be obtained from the difference between the time the attack was detected and the time the notification reached the administrator via Telegram bot. Integration with Telegram allows administrators to receive real-time notifications, enabling them to act faster. Fail2ban's implementation integrated with Telegram notifications proved effective in improving server security. The system is not only able to detect and block attacks and ensures that administrators are immediately notified of threats. This integration is recommended for organizations seeking to improve their security threat response. As a network administrator, he/she should be responsible for network traffic on the server; thus, it is mandatory to monitor and maintain the security of the server network so that it runs safely without interruption. Based on the obtained problems, it is necessary to develop a development that considers recording activities or logs to detect attacks on the server. If an attack activity is detected, a warning message will appear on the corresponding Telegram. Telegram is used because it can be used on various devices; thus,

The network administrator server can use any device installed with Telegram to obtain a warning message during an attack. There is also a bot feature that can be used for information automation, which will make it easier for users. The focus in this development is to integrate to detect attacks that will appear in the form of warning messages that will be sent to the Telegram Bot conducted by Fail2ban. Thus, it can be concluded that the purpose of this study is to meet the needs of the network administrator server in maintaining the network security system on the server by securing it with the Fail2ban configuration to detect an attack and send a warning message to Bot Telegram.

4. CONCLUSION

In addition, testing against Brute force attacks poses a considerable risk to web servers, with potentially severe consequences. Implementing strong preventive measures, continuous monitoring, and leveraging Telegram notifications for real-time alerts significantly improved the organization's security posture. These combined efforts ensure robust and responsive detection of brute force attacks. Fail2ban was able to quickly discover the IP address from which the attacker performed the brute force attack and took preventive action by blocking the attacker's ip for 3 failed login attempts within a specified time limit of 3600 s.

It is thus concluded that: (1) Brute force attacks pose a great risk to web servers and can lead to serious consequences if not handled properly. The implementation of strong precautions, such as blocking IPs after multiple failed logins, is important to protect the server from attacks. (2) The use of real-time notifications via Telegram speeds up the response to threats and improves the efficiency of attacks. (3) The combination of rapid detection and effective countermeasures, such as IP blocking using Fail2ban, strengthens an organization's overall security posture; Fail2ban can detect an attacker's IP after three failed login attempts and block it within the specified time (3600 seconds), preventing further attacks.

5. REFERENCES

[1] D. Y. Kao; E. C. Chang, and F. C. Tsai, "Extracting Suspicious IP Addresses from WhatsApp Network Traffic in Cybercrime Investigations," Int. Conf. Adv. Commun. Technol. ICACT, vol. 2019-Febru, no. 1, pp. 1108–1115, 2019, doi: 10.23919/ICACT.2019.8701941.

[2] Z. T. Sworna, Z. Mousaviand M. A. Babar, "NLP methods in host-based intrusion detection systems: A systematic review and future directions," J.

Netw. Comput. Appl., vol. 220, no. November 2022, p. 103761, 2023; doi: 10.1016/j.jnca.2023.103761.

[3] K. Razikin and B. Soewito, "Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework," Egypt. Informatics J., vol. 23, no. 3, pp. 383–404, 2022, doi: 10.1016/j.eij.2022.03.001.

[4] R. Ramadhan, J. Latunyand S. J. Litiloly, "Perancangan Pengamanan Server Apache Menggunakan Firewall Iptables Dan Fail2Ban," vol. 0, no. 0, pp. 9–15, 2022.

[5] K. A. Prasetyo, M. Idhomand H. E. Wahanani, "Pada Multiple Server Dengan Menggunakan," vol. 1, no. 3, pp. 789–796, 2020.

[6] D. SyaifuddinRisqiwati, and E. A. Irawan, "Realtime Pencegahan Serangan Brute Force dan DDOS Pada Ubuntu Server," Techno.Com, vol. 17, no. 4, pp. 347–354, 2018, doi: 10.33633/tc.v17i4.1766.

[7] A. R. Hakim, J. Rinaldi, and M. Y. B. Setiadji, "Design and Implementation of NIDS Notification System Using WhatsApp and Telegram," 2020 8th Int. Conf. Inf. Commun. Technol. ICoICT, 2020. pp. 3–6, 2020. doi: 10.1109/ICoICT49345.2020.9166228.

[8] B. Wibowo, "Smart Home Security Analysis Using Arduino Based Virtual Private Network".

[9] M. Sulthan, A. Rahmatullah, A. Muhandhatul Nabila, S. S. Dewi, V. Datryand F. A. Azaruddin, "Implementasi SIEM dan IDS Dalam Monitoring Terhadap Ancaman Serangan Pada WEB Server," vol. 2, no. 1, pp. 130–137, 2024, [Online]. Available: https://doi.org/10.59841/saber.v2i1.666

[10] D. Kusuma, U. Darussalam, and D. Hidayatullah, "Implementasi Monitoring Jaringan Melalui Aplikasi Sosial Media Telegram Dengan Snort," J I M P - J. Inform. Merdeka Pasuruan, vol. 5, no. 1, pp. 6–9, 2020, doi: 10.37438/jimp.v5i1.242.

[11] T. Hidayat, "Internet of Things Smart Agriculture on ZigBee: A Systematic Review," J. Telekomun. Dan Komput., vol. 8, no. 1, p. 75, 2017, doi: 10.22441/incomtech.v8i1.2146.

[12] A. T. Zy, A. R. Widyaand D. Taryana, "Analisa Keamananan Server Iot," no. September 2019.

[13] Stefan Stanković, Slavko Gajin, and Ranko Petrović, "A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis," IX Int. Conf. IcETRAN, vol. IX, no. June, pp. 6–9, 2022.

[14] A. Yuswanto and B. Wibowo, "a Systematic Review Method for Security Analysis of Internet of Things on Honeypot Detection," Teknokom, vol. 4, no. 1, pp. 16–20, 2021; doi: 10.31943/teknokom.v4i1.54.

[15] M. B. Khan, "Advanced Persistent Threat: Detection and Defense," 2020, [Online]. Available: http://arxiv.org/abs/2004.10690

[16] H. Wang, H. He, W. Zhang, W. Liu, P. Liu, and A. Javadpour, "Using honeypots to model botnet attacks on the internet of medical things," Comput. Electr. Eng., vol. 102, no. January, p. 108212, 2022, doi: 10.1016/j.compeleceng.2022.108212.