Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 06, June - 2024

Developing Proactive Cyber Threat Defense Systems on Server Computers Using Honeypot Techniques

Kit Sringendee, Prasong Praneetpolgrang, Surasak Mungsing

Information Technology Program
Faculty of Information Technology
Sripatum University, Bangkok, Thailand

***Abstract*— This research focuses on proactive cyber threat prevention on server computers using honeypot and bait techniques. The objective is to anticipate and intercept unauthorized attempts to guess usernames or passwords to gain access to the server computers. In this study, honeypots and bait techniques were used to simulate the services of an organization's server computer, which can be accessed from any public network. The developed system collects data on activities and events from these honeypots mechanisms, analyzes this data, and generates protective conditions based on the findings. These conditions are then compared with newly defined parameters. When the system detects a match with these predefined conditions, it immediately acts to prevent cyber threats to the server computer. The primary goal is to halt ongoing cyber attacks on the server computers and continuously monitor and manage the server computers in case of repeated cyber intrusions.**

***Keywords*— Honeypot, Analyzes, Server**

I. INTRODUCTION

Currently, Security Information and Event Management (SIEM) systems are utilized to address cybersecurity issues by collecting event data from various sources and analyzing it to detect abnormal activities. Integrating SIEM with honeypot techniques is particularly intriguing. Additionally, studying attacks on Honeypots helps system administrators understand these attacks and develop further defenses. According to the research by Anil Tom and MN Nachappa [1], honeypots are crucial for detecting and analyzing malicious network traffic. Implementing SIEM enhances the monitoring, analysis, and alerting of threats to organizational server computers.

Given the issues, the researcher has devised new methods to protect against potential Brute-Force Attacks on the server. This research focuses on the SIEM and details as follow:

1. Analyze cyber threats on server computers using honeypots.
2. Develop a system to prevent Brute Force Attacks on server computers.
3. Evaluate the effectiveness of the cyber threat prevention system against Brute Force Attacks.

II. MOTIVATION

Implementation of Security Information and Event Management Systems.

The use of Security Information and Event Management systems involves the installation of both a central server and monitoring servers. This comprehensive setup allows for detailed system log inspection to identify activities on servers providing internet services. When anomalies meeting predefined criteria are detected, the SIEM system, following administrator-defined commands, initiates actions on the relevant servers.

To facilitate immediate response, the SIEM system utilizes an Application Programming Interface (API) to send commands to servers equipped with pre-configured command programs. Subsequent actions are meticulously monitored through system logs to ensure rapid and accurate responses to potential security threats. This integration creates a dynamic and automated security infrastructure, enhancing the resilience and overall responsiveness of the server systems.

III. METHODOLOGY

A. Literature Review of Relevant Concepts and Theories

1. Operation of SIEM in receiving Log System data from the server.
2. Storing Log System data generated by Honeypots [2] to capture threat activities on the server.
3. Reading Log System data written in JSON format to identify the generated rule.id and MITRE ATT&CK values [3] to detail the nature of the attacks.

The SIEM system [4] utilized by the researcher to detect Brute-Force Attack cyber threats is an open-source solution called Wazuh [5]. The Wazuh Server operates in conjunction with the Elastic Stack [6]. When an event occurs on a server computer, the Agent program (bests) installed on the server computer copies the Log System data and sends it to the SIEM. The data is processed in Logstash and then stored in Elasticsearch [7] in JSON format. The system compares the obtained Log values with the rule.id values configured in the SIEM to match the events with specific rule.ids. Fig. 1.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 06, June - 2024

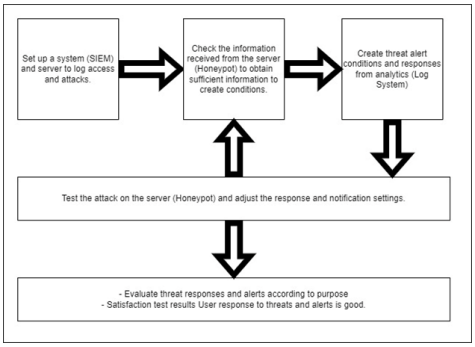

Fig. 1. Research Conceptual Framework

The SIEM system, as described above, allows the Log System on the server computer with the installed Agent to receive various commands. These commands can direct actions such as protecting the server computer or executing specified instructions.

The researcher installed an Agent to collect Log System data from the server computer used as a Honeypot, allowing access from public networks or the internet. This research, the installation was performed on AWS Cloud Services.

Fig. 2. Log System from Honeypot

Fig. 2 illustrates the log data stored during the period from March 16th, 2024 at 00:00 hours to April 15th, 2024 at 23:30 hours. It can be observed that there was a total of 35,968 log entries during this timeframe. Upon analysis by the researchers, it was found that the attacks primarily consisted of SSH Access attempts using the username "Root," corresponding to rule.id = 5760, as depicted in Fig. 3.

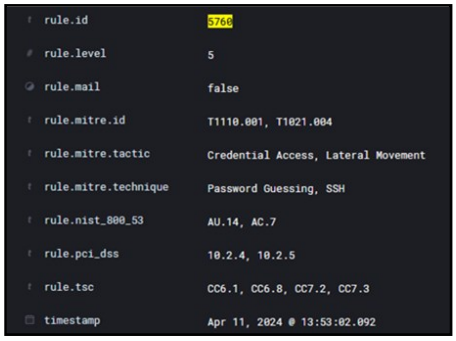

Fig. 3. rule.id 5760 is Credential Access

By selecting only, the entries with rule.id = 5760, which represents attempts to access the network computer via SSH with incorrect passwords, it was found that there were a significant number of occurrences, totaling 3,287 instances. This indicates a notable attempt at Brute Force Attack. Hence, the value of rule.id 5760 was utilized to establish new conditions for preventing such attacks on the network computer. It can be observed that there were attempts to access the network computer via SSH, as indicated by the MITRE ATT&CK technique, and confirmed by the rule.id value of 5760. This ID can be utilized to formulate conditions within the rule set of the SIEM.

B. Utilizing Log System from Honeypot to Establish Conditions and Test Protection Mechanisms

1. Creating a new rule.id in the SIEM system in .xml file. Develop a new rule.id within the SIEM system's rules using an .xml file. This rule should employ the MITRE ATT&CK framework and trigger when the cumulative count exceeds four occurrences, thereby initiating a defense mechanism against Brute Force attacks.
2. Testing the new rule.id condition created in the .xml file. The new rule.id should be tested against an SSH Brute Force attack. If an IP address attempts to randomly guess passwords four times within a 10-minute interval, the system should immediately block that IP address.
3. Setting drop packet Intervals in SIEM parameters. Configure the system to drop packets at specified intervals according to the SIEM system parameters. When researchers obtain data from Step 1, it becomes evident that incorporating rule.id 5760 as a new condition ensures that repeated SSH Brute Force attacks, reaching four attempts within 600 seconds, will be logged in the SIEM system as rule id = 100030.

The intrusion detection system was tested using the Nmap program, a programmatic scanning tool, to assess its ability to detect brute force attacks attempting to gain unauthorized access to the network computer via SSH. Nmap was employed to conduct password guessing attacks, simulating a brute force attack scenario. This testing of the intrusion detection system's effectiveness serves to ensure the security of the network computer before deploying it into a public network environment.

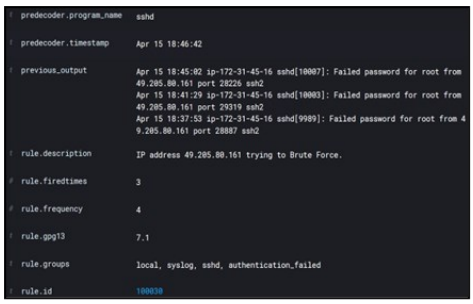

Fig. 4. Log detail rule id 100030 in SIEM

Implementation and Testing of the System in a Real-World Scenario. Fig. 4, it is observed that there were attempts to access the server via SSH [8], as defined by the set conditions. The researchers utilized these parameters to prevent SSH Brute Force attacks. By configuring rule.id in the SIEM system, the researchers established conditions that log rule.id 100030 when such attempts occur.

Having successfully recorded and displayed rule.id 100030 in the SIEM, the researchers designed a process where the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 06, June - 2024

SIEM sends commands to protect the main server through an installed agent, as demonstrated in Fig. 5.

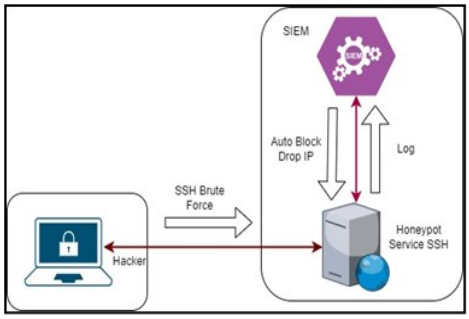

Fig. 5. Flow System Diagram

C. Evaluation of the Effectiveness of Cyber Attack Prevention on Main Server Against Brute Force Attacks

The effectiveness of the cyber-attack prevention system against Brute Force Attacks on server was evaluated using an event response analysis technique based on predefined conditions. This evaluation employed a 5-level (Likert) [9] rating scale to interpret the effectiveness in terms of accuracy and speed, as follows level of effectiveness.

- A score of 4.21 – 5.00 indicates the highest.
- A score of 3.41 – 4.20 indicates a high.
- A score of 2.61 – 3.40 indicates a moderate.
- A score of 1.81 – 2.60 indicates a low.
- A score of 1.00 – 1.80 indicates the lowest.

IV. RESEARCH RESULTS

A. Results of Cyber Threat Analysis on Honeypot Server

The analysis of cyber threats on honeypot servers [10] reveals various forms of insights:

- Attack Patterns
  The analysis of threats on honeypots enables administrators to understand common attack patterns, which can directly aid in preventing attacks on operational systems.
- Attacker Types
  Threat analysis also helps identify the types of attackers targeting honeypot servers. This understanding is crucial for developing appropriate counter-strategies and defenses.
- Vulnerabilities and Risks
  Through threat analysis, vulnerabilities and risks that honeypot servers might have can be identified. This information is instrumental in enhancing the security of operational systems.
- Attack Data and Techniques
  Managing the data and techniques gleaned from threats can be used to train and improve the skills and understanding of involved personnel, such as system administrators and software developers.

Honeypots are used to gather information about potential attackers and serve as valuable tools in bolstering the security of computer systems. They allow administrators to understand and effectively respond to attacks. Research by Stefan Machmeier [11] highlights that honeypots are employed to collect data on attackers by simulating vulnerable targets in cloud environments, aiming to improve security infrastructure.

B. Results of Developing a Cyber Threat Prevention System on Main Server Computers Against Brute Force Attacks Using Event Response Analysis Techniques

The development of a cyber threat prevention system on server [12] against Brute Force Attacks using predefined event response analysis techniques reveals that when an attack occurs, the SIEM compares it with the MITRE ATT&CK Framework. The SIEM then records and identifies the attack technique as Password Guessing [13], SSH, which constitutes a Brute Force Attack, and assigns it rule.id = 5760 as shown in Fig. 6.

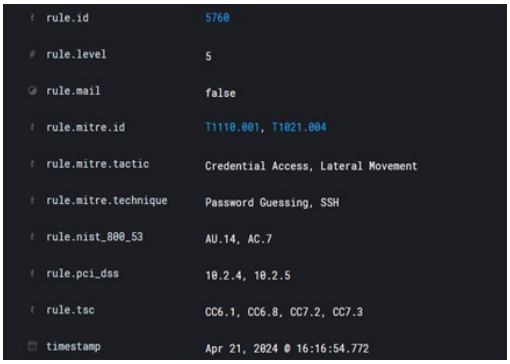

Fig. 6. Detail rule.id 5760

When researchers applied the MITRE ATT&CK values indicating rule.id = 5760 in the SIEM to define rules in the .XML file format within the Rule section of the SIEM, the following procedure was established.
If rule.id = 5760 is detected four times within 600 seconds from the same source IP, it should be identified as "trying to Brute Force" and assigned rule id = "100030" as illustrated in Fig. 7. This rule is then recorded in the SIEM to serve as a trigger for responding to the main server when this condition arises.

```
<group name="local,syslog,sshd,">
  <rule id="100030" level="10" frequency="4" timeframe="600">
  <if_matched_sid>5760</if_matched_sid>
  <same_source_ip />
  <description>IP address $(srcip) trying to Brute Force.</description>
  <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,gpg13_7.1,</group>
  </rule>
</group>
```

Fig. 7. Conditions for analyzing Brute Force Attack

Researchers utilized the value rule.id = 100030 as a condition in configuring the parameters for response in the Configuration section of the SIEM. This configuration aims to execute commands located within the Active-response section of the SIEM.
Specifically, under the name "firewall-drop" the server computer is instructed to block packets from the IP addresses falling under the condition of rule.id = 100030 for a specified duration of 30 minutes, as detailed in Fig. 8.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 06, June - 2024

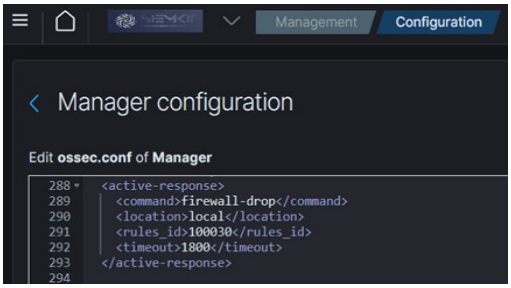

Fig. 8. Conditions for Response Brute Force Attack

Following the process, when the testing for attacks reaches the predefined conditions, the SIEM records the attacks in its log. This logging mechanism enables the SIEM to notify administrators of attempted Brute Force Attacks on the main server computer, displaying rule number 100030, as depicted in Fig. 9.

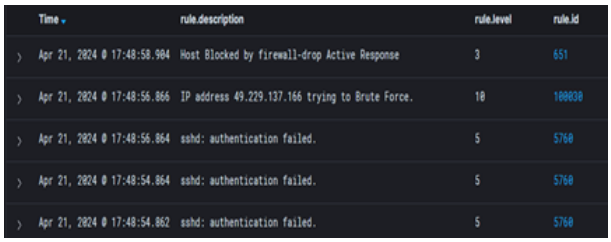

Fig. 9. Log brute force attack and block IP

The blocking of the IP address originates from the public IP attempting a Brute Force Attack on the main server, which acts as a honeypot for testing attack prevention. Researchers implemented attack prevention by blocking the IP address of the attacker, preventing access to the main server computer. Upon detection of the Brute Force Attack, the SIEM sends commands to the honeypot to suspend access to the main server computer on the network. The IP address from the public IP source is blocked for a period of 30 minutes, as specified for testing attack prevention measures and to demonstrate the effectiveness of the predefined conditions, as shown in Fig. 10.

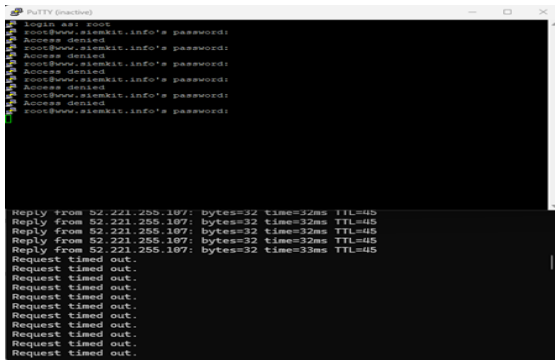

Fig. 10. Active response block IP

C. Evaluate the effectiveness of cyber threat prevention

The server acting as a honeypot against Brute Force Attacks, analysis, and notification performance were measured and compared with the detection conditions for Brute Force Attacks recorded in the SIEM. The results are as follows.
The testing for attacks was divided into 5 sets. In each testing set, attempts to access the server via SSH were made 4 times or more. The analysis of the log recordings with rule.id = 100030 and the effectiveness of prevention measures were observed. The average performance was found to be at the highest level ($\bar{x}$ = 5.00) when analyzing Brute Force Attacks and implementing prevention measures by dropping IP addresses, as follows:

- Number of attempts: 4 or more.
- Detection condition: rule.id = 100030.
- Prevention measure: Drop IP.

These conditions resulted in the highest average effectiveness level, demonstrating optimal performance in detecting and preventing Brute Force Attacks. The analysis and prevention effectiveness based on failed login attempts are categorized as follows:

- After 4 failed login attempts are level 5.
- After 5 failed login attempts are level 4.
- After 6 failed login attempts are level 3.
- After 7 failed login attempts are level 2.
- After 8 failed login attempts are level 1.

These ratings reflect the system's efficiency in detecting and responding to Brute Force Attacks, with the highest effectiveness achieved when responses were triggered after 4 failed login attempts.

Table I Attack protection test results Brute Force Attack Levels.

Test No.	Analyzation	Drop IP	$\bar{x}$
No.1	5	5	5
No.2	5	5	5
No.3	4	4	4
No.4	5	5	5
No.5	5	5	5

Table 1 presents the test results showing the effectiveness of attack analysis and prevention. The researchers tested the prevention measures based on the log condition rule.id 100030 by simulating access to the main server computer via SSH, where the user is Root and enters an incorrect password four times. This scenario meets the set rule condition and constitutes one test set. A total of 5 test sets were conducted. The test results are detailed in Table 1. Across the 5 test sets, the analysis of log records with rule.id = 100030 and the prevention measures showed an average effectiveness at the highest level ($\bar{x}$ = 5.00). This was determined by the time taken to analyze the Brute Force Attack and display the values in the SIEM system's event log Fig. 11.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 06, June - 2024

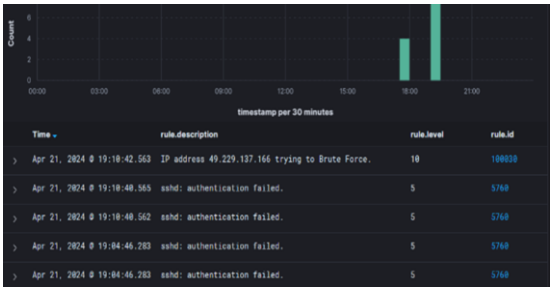

Fig. 11. Log Recording

V. CONCLUSION

This research analyzes threats to main server computers using a SIEM [14], [15], [16], which can store log data from honeypot server computers. The logs generated from various events are analyzed using rule.id 100030 to understand the attacks and to establish additional rules and conditions. These rules can then be used to automate the prevention of Brute Force Attacks. When a threat event matches the predefined parameters on the main server computer, the system can be further developed to enhance cyber threat prevention efficiently. This approach also serves as a testing mechanism for main server protection before deployment in real-world scenarios.

The researchers analyzed threats to the server computer by storing log data and defining additional conditions to monitor Brute Force Attacks. When threat events match the predefined parameters, the system can effectively detect and prevent attacks. This enhances the efficiency of cyber threat prevention, aligning with the findings of Abdullah Almurayh [17], who studied password cracking using Brute Force and Dictionary Attack algorithms. They found that Brute Force attacks can be sped up by 4.4 times. Using a SIEM for real-time or near-real-time server protection significantly enhances the effectiveness of cyber threat prevention and ensures readiness to counter threats at any time.

VI. FUTURE RESEARCH

This research focuses on the development of a proactive cyber threat prevention system for network computers by employing raps and bait techniques.

A. Implementation Recommendations for Practical Application

Utilize the research outcomes for practical application to uphold the cybersecurity of network computers providing external access within organizations, which remains crucial for institutions such as educational establishments, small and medium-sized enterprises (SMEs), and governmental agencies. Despite budget constraints in cybersecurity maintenance, particularly for open-source solutions devoid of licensing costs, the ease of implementation and absence of financial limitations render them advantageous for organizations operating under budgetary constraints.

B. Future Research Considerations

Future research should consider the use of Security Information and Event Management (SIEM). Relying solely on SIEM for detecting and preventing Brute Force Attacks may be insufficient. However, SIEM can be further developed to protect against other types of server attacks, such as ransomware, malware, or Distributed Denial of Service (DDoS) attacks. SIEM can read data from log systems and detect activities on the server computer. If suspicious or abnormal activities are detected, artificial intelligence technology can be employed to analyze the data from the SIEM. This can aid in the detection and prevention of attacks by providing recommendations for mitigation, containment, or system recovery.

REFERENCES

[1] A. Tom and M. N. Nachappa, “A Study on Honeypots and Deceiving Attackers using Modern Honeypot Network,” International Journal of Trend in Scientific Research and Development (IJTSRD), vol. 5, no. 1, Nov.-Dec. 2020.

[2] S. Bhanu, G. Khilari, and V. Kumar, “Analysis of SSH attacks of Darknet using Honeypots,” International Journal of Engineering Development and Research, 2013.

[3] ATT&CK M., “Versions of ATT&CK,” 2023. [Online]. Available: https://attack.mitre.org/resources/versions. [Accessed: Oct. 16, 2023].

[4] A. Tariq, J. Manzoor, M. Aziz, Z. U. A. Tariq, and A. Masood, “Open source SIEM solutions for an enterprise,” Information & Computer Security, vol. 31, no. 1, pp. 88-107, 2022.

[5] T. Suryantoro, B. Purnomosidi, and W. Andriyani, “The Analysis of Attacks Against Port 80 Webserver with SIEM Wazuh Using Detection and OSCAR Methods,” in Proc. 2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Dec. 2022, pp. 8-9.

[6] C. Yu, K. Congwang, L. Jian, W. Huimei, and X. Ming, “A network attack detection system of OpenStack cloud platform based on Elastic Stack,” Proc. SPIE 12172, International Conference on Electronic Information Engineering and Computer Communication EIECC 2021, Dec. 2021.

[7] Yudhistira, A., & Fitrisia, Y, “Monitoring Log Server dengan Elasticsearch Logstash dan Kibana (ELK),” RABIT: Jurnal Teknologi dan Sistem Informasi Univrab, 8(1), 124-134, 2023.

[8] Z. P. Chen and T. M. Khan, “Analysis of SSH Honeypot Effectiveness,” Advances in Information and Communication, Proc. 2023 Future of Information and Communication Conference (FICC), vol. 2, pp. 759-782, 2023.

[9] S. Yurat, “Why Likert,” Journal of Innovation and Management, Research Promotion and Development Center, Sripatum University, 2022. (in Thai)

[10] D. Zielinski and H. A. Kholidy, “An Analysis of Honeypots and their Impact as a Cyber Deception Tactic,” State University of New York (SUNY) Polytechnic Institute, College of Engineering, Network and Computer Security Department, Utica, NY, USA, Dec. 30, 2022.

[11] Machmeier, S. “Honeypot Implementation in a Cloud Environment.” Faculty of Mathematics and Computer Science, Heidelberg University, 2023.

[12] D. P. Zegzhda, D. S. Lavrova, E. Pavlenko, and A. A. Shtyrkina, “Cyber Attack Prevention Based on Evolutionary Cybernetics Approach,” Symmetry, vol. 12, no. 11, p. 1931, Nov. 2020.

[13] C. Liu, G. D. Clark, and J. Lindqvist, “Guessing Attacks on User-Generated Gesture Passwords,” Rutgers University, vol. 1, no. 1, pp. 3, Mar. 2017

[14] V.-M. C., “SIEM. Security Information and Event Management Solutions Implementation in Private or Public Clouds,” Scientific Bulletin of Naval Academy, 2016.

[15] B. Filkins, “An Evaluator's Guide to NextGen SIEM,” SANS Institute, 2019.

[16] G. Granadillo, S. Gonzalez-Zarzosa, and R. Diaz, “Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructure,” Sensors, vol. 21, no. 14, pp. 4759, 2021.

[17] A. Almurayh and N. Min-Allah, “Password Cracking with Brute Force Algorithm and Dictionary Attack Using Parallel Programming,” Applied Sciences, vol. 13, no. 10, pp. 5979-5979, 2023.