Jurnal Pertahanan: Media Informasi tentang Kajian dan Strategi Pertahanan yang Mengedepankan Identity, Nasionalism dan Integrity
Vol. 9 No. 3 (2023) pp.580-591
https://jurnal.idu.ac.id/index.php/DefenseJournal

# TELER Performance as Real-Time Intrusion Detection and Threat Alert Based on Web Log-In Detecting Directory Bruteforce Attacks on Websites

**Rio Darmawan[1*], Bita Parga Zen[2], Riyanti Yunita Kisworini[3]**
[1,2]Institut Teknologi Telkom Purwokerto, Indonesia
[3]STMIK Widya Utama, Indonesia

18102283@ittelkom-pwt.ac.id[1*], 1bita@ittelkom-pwt.ac.id[2*], rianti@swu.ac.id[3]
*Corresponding Author

**Article Info**

**Article history:**
Received: October 31, 2023
Revised: December 22, 2023
Accepted: December 31, 2023

**Keywords:**
Bruteforce,
IDS,
TELER,
Threat Alert
Webserver

**DOI:**
http://dx.doi.org/10.33172/jp.v9i3.19305

**Abstract**

TELER is a real-time intrusion detection and weblog-based alerting tool that runs on the terminal. TELER is designed to be a fast terminal-based threat analyzer. The IDS (intrusion detection system) is needed to help web administrators secure their servers. This study aims to test the TELER performance as real-time intrusion detection and threat alert. This study tries to implement an open-source application called TELER based on Golang. The IDS testing method on the web server this time uses directory brute force with the result that TELER can detect an attack and provide prompt notification to the web administrator when an attack occurs on the web server. The result of this study shows that the TELER successfully sent notifications to the Telegram, Discord, and Slack applications when an attack or intrusion occurs. Based on the experiments conducted in this study, Slack is the most effective application for receiving directory brute-force attack notifications. The average time for Slack to receive attack information is 0.03 seconds. TELER was successfully proven to detect cyberattacks.

2549-9459/Published by Indonesia Defense University. This is an open-access article under the CC BY-NC license (https://creativecommons.org/licenses/by-nc/4.0/).

## INTRODUCTION

War is an important thing that is necessary for each country to defend the territory, as it can be a deterrent factor against the opposing war effort. In the modern era, war is no longer made by the truce, but it has been more referring to technology, politics, and the economy. For example in World War I and II, what triggered conflicts were the struggle for territorial power, control of natural resources, advances in weaponry technology, and so on. The losses suffered as a result of World War I and II were enormous, including millions of people who died in wars, epidemics, famine, including

material losses. Therefore, the defense and security of the country are very important, so that they do not become the target of other countries to be conquered (Hidayat, Thamrin, & Widayatno, 2022).

Advances in information technology and cyber defense systems are currently developing rapidly with technological advances in the cyber field, especially on web servers and databases, which can be a threat to data and information theft, so there is a need for a security assessment to prevent data theft (Zen, Gultom, & Reksoprodjo, 2020). The positive impact of today's virtual world makes it easier for humans to develop world technology with all forms of creativity. However, the negative impact cannot be avoided (Akram & Kumar, 2017). Web servers and web-based applications are now widely used in various organizations and businesses and are often the target of multiple attacks that can cause damage to existing systems. To reduce the risk of attacks on the web, web developers need to develop secure applications to prevent attacks. Attack detection is critical to responding to incidents, limiting damage from attacks, preventing attacks, and preventing the future (Anggarini, Zen, & Pranata, 2022).

According to a report by the State Cyber and Signal Agency (BSSN), there were 290.3 million cyber attacks (intrusions) on internet networks in Indonesia. The biggest attack is a data test attack, followed by attacks using malware methods. Compared to many cyber attacks, the number of complaints from the public regarding the incident is relatively small. Cyber attacks in Indonesia spiked in September, and October and declined sharply in November. In November and December, still much higher than in the first six months of 2019. This incident is expected to involve many people in October, coinciding with the appointment of the new President and Vice President of Indonesia for the 2019-2024 period (BSSN, 2023).

Considering the broad field of cyber defense, namely, to build a sense of defense in the field of cyber security in the defense sector, the cyber defense guidelines have been prepared (Zen, Anggi, & Putro, 2022). Through the use of current information and communication technology, this encourages the formation of cyberspace. Currently, the Indonesia Ministry of Defense receives 60 to 80 thousand cyber-attacks every day in the form of Ransomware, Trojan Policy, Policy, and others. These attacks include strategic data such as Indonesian National Army personnel information such as address, and age blood group website database portal and appreciated (CNN Indonesia, 2018).

Intrusion can be defined as a collection of events and threats that threaten the confidentiality and integrity of information or data on internet resources such as user data, company data, and secret state data. Attacks on computer networks are a radical threat because they are threatened every hour of the day and with the discovery of security holes very quickly (Tedyyana, Ghazali, & Purbo, 2021)). Problems in detecting attacks are increasing due to the use of botnets by attackers. Two common network attacks are Denial of Service (DoS) and Bruteforce (Alfidzar & Zen, 2022). To handle intrusion on the server, an Intrusion Detection System (IDS) is required, which is installed on the server. The IDS will track attacks and suspicious activity on the server and then send a report to the security system administrator (Tabash, Allah, & Tawfik, 2020). In intrusion detection, web-based applications usually use weblogs from the web server to detect intrusions. It is very useful for web administrators to be able to find out the cause of attacks on web servers. By analyzing this log file, the web administrator can classify several attack patterns on the web (Ma, Jiang, Dong, Jia, & Li, 2017).

This study uses different software, namely TELER. TELER is a real-time intrusion detection and weblog-based alerting tool that runs on the terminal. TELER is designed to be a fast terminal-based threat analyzer. The core idea is to quickly analyze and classify

threats to prevent future hazards more quickly (Tedyyana, Ghazali, & Purbo, 2021) TELER is a Go HTTP middleware that provides TELER IDS functionality to protect against web-based attacks and improve the security of Go-based web applications. It is highly configurable and easy to integrate into existing Go applications and the TELER was designed to be a fast, terminal-based threat analyzer. Its core idea is to quickly analyze and hunt threats in real time (Siswanto, 2023). Based on the explanation above, therefore, this study aims to test the TELER performance as real-time intrusion detection and threat alert.

## METHODS

### System Architecture

The data was taken using TELER and scanning the log files on the webserver /var/log/apache2/access.log. The results will detect if there are signs of dangerous requests from attackers who use brute force directory scanning on the web server. Thirty sample data were taken and an analysis was carried out whether the attack was successful in finding the directory on the web server or not. The system architecture consists of 1 PC/laptop, 1 virtual private server, and 1 mobile phone. Firstly, 1 PC/laptop will be used by the attacker to carry out the attack, secondly, the virtual private server will be used for web server media for attack testing, and then the mobile phone will be used to receive notifications when the attack occurs (William, Choubey, Chhabra, & Bhattacharya, 2022). The system architecture can be seen in Figure 1.

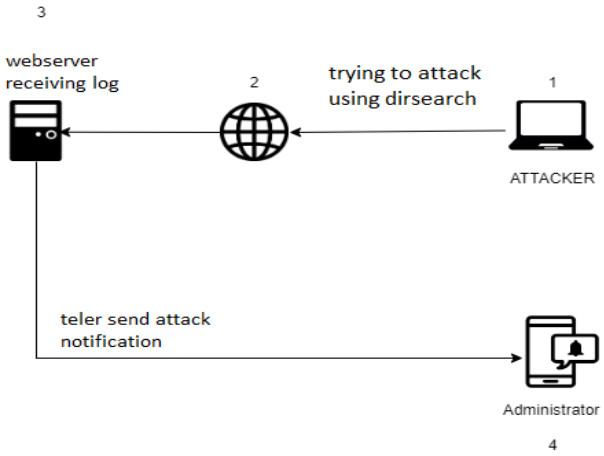
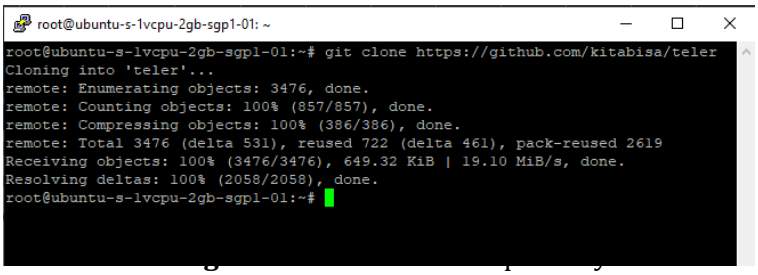



**Figure 1**. System Architecture

In Figure 1 can be seen that the webserver architectural design uses Apache2, Damn Vulnerability Web Application (DVWA) and TELER. The attacker's PC, the dirsearch application is installed which acts as the perpetrator of the attack using the brute force method on the web server. The process of installing the TELER tools with the command "git clone https://github.com/kitabisa/TELER" on the VPS server will be used as research material for testing directory brute force attacks (Tedyyana, Ghazali, & Purbo, 2021). It is needed to make sure to set UP Golang to run this TELER tool as can be seen in Figure 2.




In the next step, we must configure the TELER file section called TELER.yaml and adjust the log usage with the webserver used by the server. Because each web server has a different log. The Apache2 and the configuration should adjust the Apache2 log as can be seen in Figure 3.

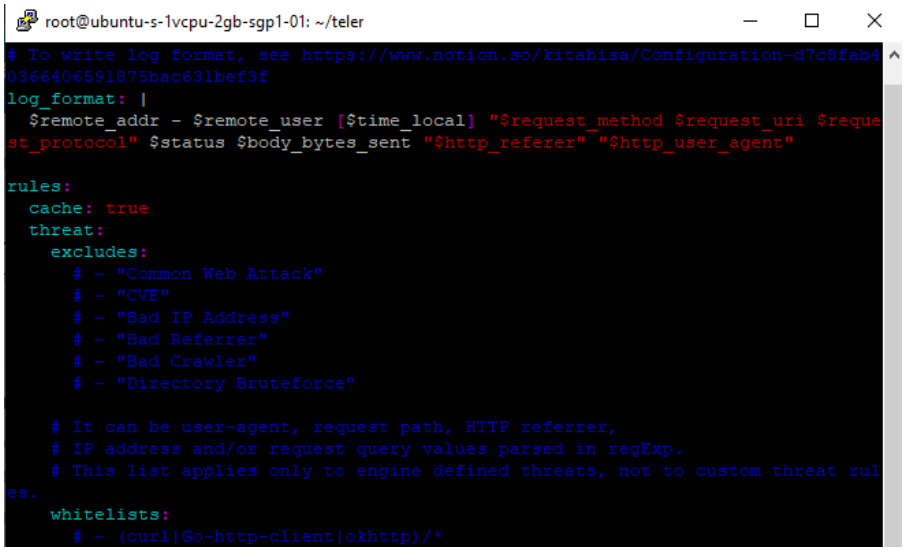



**Figure. 3** Configure the Log Format on TELER

In the next step, before running TELER, firstly must configure the alert that will be used as a medium for receiving attack information. 3 types of bots used in this step, namely Telegram, Discord, and Slack. Those three bots will be tested to see which is the most effective for receiving attack information from TELER tools. An example of writing a bot authentication token can be seen in Figure 4.

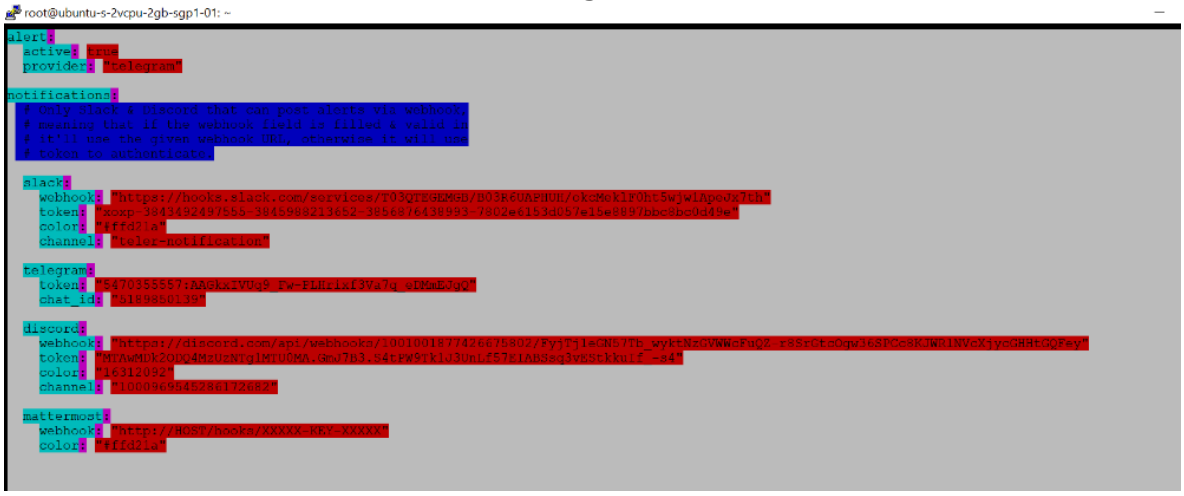



**Figure. 4** Bot authentication configuration

## Testing Directory Bruteforce Attack Using Dirsearch

Before starting the attack, first, must run TELER with the command "tail -f /var/log/apache2/access.log | TELER". This is needed, so the TELER can run continuously to see file changes as can be seen in Figure 5. To see the performance of TELER as a real-time intrusion detection and threat alert. The experiment should be conducted with directory brute force scanning using the Dirsearch application as can be seen in Figure 6.

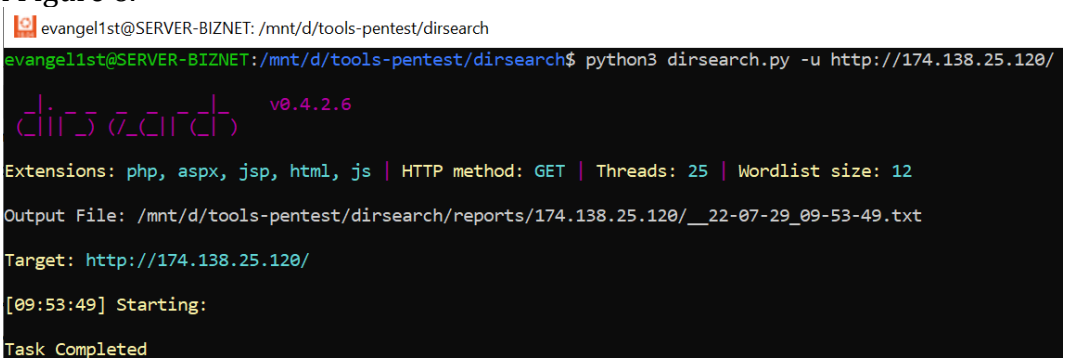



**Figure. 6** Attack Stage Using Dirsearch

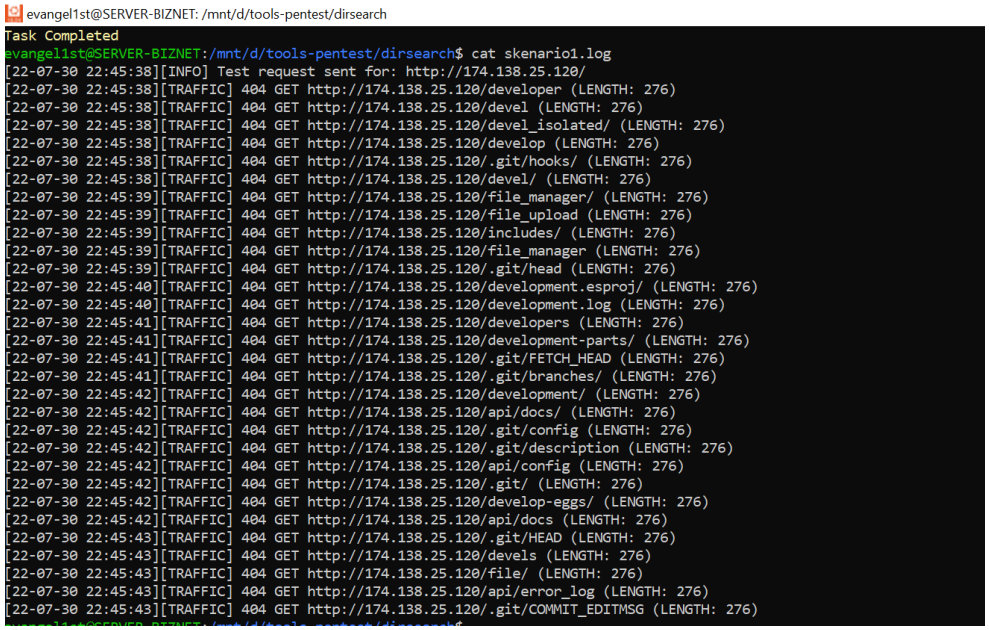



**Figure. 7** Log Attack stage Using Dirsearch

## RESULT AND DISCUSSION

This action includes evaluating the results of experiments on attacks, the detection process, and receiving attack notifications to prevent data theft in the context of state protection. This study conducted a system test to understand how to detect brute force attacks against webserver directories configured in an intrusion detection system using the TELER application. After collecting trial data, each scenario will be compared to assess its effectiveness. When TELER detects an attack, an attack notification will be received immediately as a preventive measure to maintain state data security. In addition, these steps are designed to optimize the response to attacks by identifying patterns and signs of attacks that can compromise data security. This system testing aims to increase resistance to attacks that have the potential to harm system integrity, especially in the face of brute force attacks against the webserver directory.

Applying configuration to an intrusion detection system, as carried out in this research, is a proactive effort to prevent data theft. Attack notifications generated by TELER are essential to triggering a quick and effective response from the authorities. In addition, test data analysis is critical to improving the intelligence of intrusion detection systems so they can identify attacks more accurately and strengthen defenses against data security threats. By continuing and updating prevention methods based on research results, these steps can become a solid foundation for maintaining the security of state data from the danger of theft, which is increasingly sophisticated and continues to grow.

**Log Timestamps on TELER When a Directory Brute Force Attack Occurs**

Suspicious activities and attacks on a system security or server will be recorded. Some critical information that can be dialed from this note is the activity of Paya on July 30, 2022, Mixing Wiga in the weir 49:16. This shows an effort to accept directory or desired files by trying various password combinations or names. The recommended actions involve further security reviews and continuing the security rental. Additional monitoring and reporting of this attack activity to the system administrator or security team can be the necessary steps.

**Table 1.** Log Timestamp TELER

| | | | |
|---|---|---|---|
| 30/Jul/2022:23:49:11 +0700 | 182.253.131.119 | Directory Bruteforce | /.Xe7WPM |
| 30/Jul/2022:23:49:12 +0700 | 182.253.131.119 | Directory Bruteforce | /ipch/ |
| 30/Jul/2022:23:49:12 +0700 | 182.253.131.119 | Directory Bruteforce | /local_conf.php.bak |
| 30/Jul/2022:23:49:12 +0700 | 182.253.131.119 | Directory Bruteforce | /is-bin/ |
| 30/Jul/2022:23:49:12 +0700 | 182.253.131.119 | Directory Bruteforce | /iradmin |
| 30/Jul/2022:23:49:12 +0700 | 182.253.131.119 | Directory Bruteforce | /irj/portal |
| 30/Jul/2022:23:49:12 +0700 | 182.253.131.119 | Directory Bruteforce | /iredadmin |
| 30/Jul/2022:23:49:12 +0700 | 182.253.131.119 | Directory Bruteforce | /isadmin.php |
| 30/Jul/2022:23:49:12 +0700 | 182.253.131.119 | Directory Bruteforce | /Mercury/ |
| 30/Jul/2022:23:49:12 +0700 | 182.253.131.119 | Directory Bruteforce | /moderator/admin |
| 30/Jul/2022:23:49:12 +0700 | 182.253.131.119 | Directory Bruteforce | /mfr_admin |
| 30/Jul/2022:23:49:12 +0700 | 182.253.131.119 | Directory Bruteforce | /mesos/ |
| 30/Jul/2022:23:49:13 +0700 | 182.253.131.119 | Directory Bruteforce | /irequest/ |
| 30/Jul/2022:23:49:13 +0700 | 182.253.131.119 | Directory Bruteforce | /refresh_dblist.php |
| 30/Jul/2022:23:49:14 +0700 | 182.253.131.119 | Directory Bruteforce | /local_conf.php.bac |
| 30/Jul/2022:23:49:14 +0700 | 182.253.131.119 | Directory Bruteforce | /ip_configures/ |
| 30/Jul/2022:23:49:14 +0700 | 182.253.131.119 | Directory Bruteforce | /irc-macadmin/ |
| 30/Jul/2022:23:49:14 +0700 | 182.253.131.119 | Directory Bruteforce | /issue/createmeta |
| 30/Jul/2022:23:49:15 +0700 | 182.253.131.119 | Directory Bruteforce | /kafka/ |
| 30/Jul/2022:23:49:15 +0700 | 182.253.131.119 | Directory Bruteforce | /local_bd_new.txt |
| 30/Jul/2022:23:49:15 +0700 | 182.253.131.119 | Directory Bruteforce | /cubemail/restore.php |
| 30/Jul/2022:23:49:15 +0700 | 182.253.131.119 | Directory Bruteforce | /kairosdb/ |
| 30/Jul/2022:23:49:15 +0700 | 182.253.131.119 | Directory Bruteforce | /issues |
| 30/Jul/2022:23:49:15 +0700 | 182.253.131.119 | Directory Bruteforce | /isadmin |
| 30/Jul/2022:23:49:15 +0700 | 182.253.131.119 | Directory Bruteforce | /local_bd_old.txt |
| 30/Jul/2022:23:49:15 +0700 | 182.253.131.119 | Directory Bruteforce | /iso_admin |
| 30/Jul/2022:23:49:16 +0700 | 182.253.131.119 | Directory Bruteforce | /local_settings.py |
| 30/Jul/2022:23:49:16 +0700 | 182.253.131.119 | Directory Bruteforce | /ipython/tree |
| 30/Jul/2022:23:49:16 +0700 | 182.253.131.119 | Directory Bruteforce | /ispmgr/ |
| 30/Jul/2022:23:49:16 +0700 | 182.253.131.119 | Directory Bruteforce | /learn/cubemail/dump.php |
| 30/Jul/2022:23:49:16 +0700 | 182.253.131.119 | Directory Bruteforce | /isapi/ |

**Notification of Attacks on Telegram, Discord, and Slack Applications**

Notifications sent by TELER into the Telegram, Discord, and Slack applications that have been configured and successfully display the attack category, the request made by

the attacker, the date of the attack, the attacker's IP address, the attacker's user agent, and the status of the response code on the server.

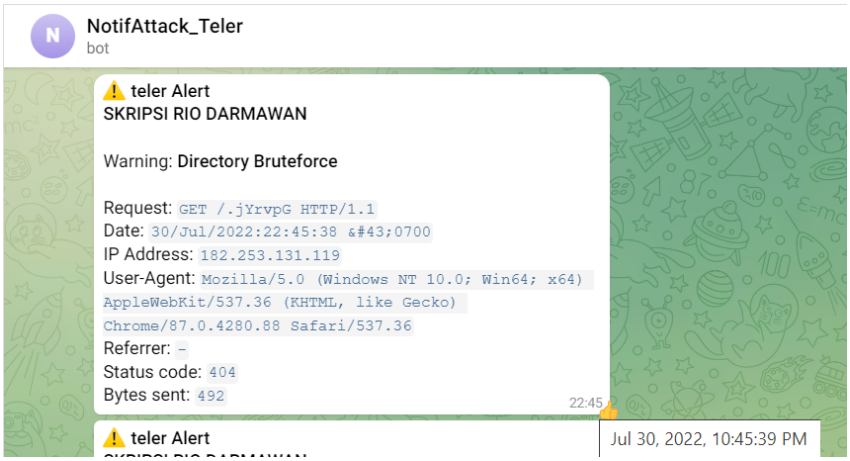



**Figure. 8** Alert Notification on Telegram

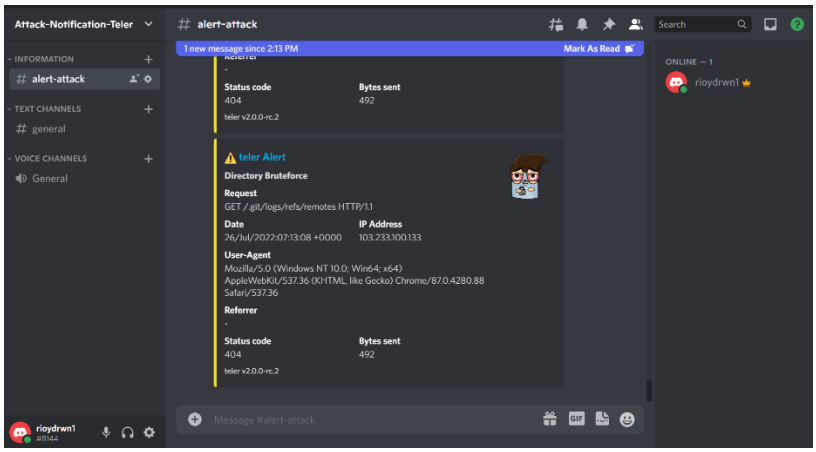



**Figure. 9** Alert Notification on Discord

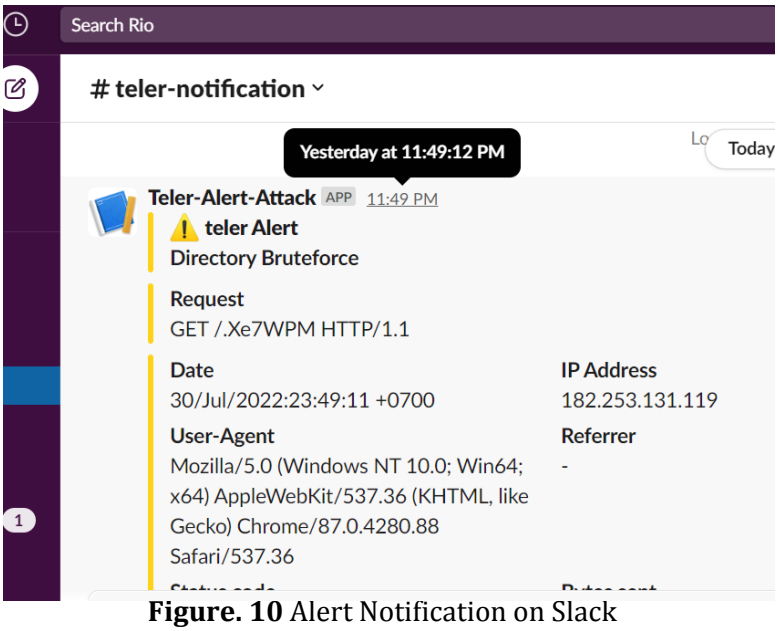



**Figure. 10** Alert Notification on Slack

## Testing Scenario

Several test scenarios are used to get the results of system performance and period as an intrusion detection system, including using Telegram, Slack, and Discord as a medium for receiving information about directory bruteforce attacks on web servers. Table 2 shows a list of scenarios used in this study.

**Table 2.** Testing Scenario

| Scenario | Scenario |
|---|---|
| Scenario 1 | Telegram as a directory bruteforce attack notification sender |
| Scenario 2 | Discord as a directory bruteforce attack notification sender |
| Scenario 3 | Slack as a directory bruteforce attack notification sender |

## Scenario 1

In Scenario 1, Telegram became the medium for receiving directory brute force attack information. Table 3 is the result of the Scenario 1.

**Table 3.** Time Attack on Telegram

| No | Attack Time | Attack Detection Time | Receive Attack Information | Receive Attack Information Period |
|---|---|---|---|---|
| 1 | 30/Jul/2022:22:45:38 | 30/Jul/2022:22:45:38 | 30/Jul/2022:22:45:39 | 1 second |
| 2 | 30/Jul/2022:22:45:38 | 30/Jul/2022:22:45:38 | 30/Jul/2022:22:45:39 | 1 second |
| 3 | 30/Jul/2022:22:45:38 | 30/Jul/2022:22:45:38 | 30/Jul/2022:22:45:39 | 1 second |
| 4 | 30/Jul/2022:22:45:38 | 30/Jul/2022:22:45:38 | 30/Jul/2022:22:45:39 | 1 second |
| 5 | 30/Jul/2022:22:45:38 | 30/Jul/2022:22:45:38 | 30/Jul/2022:22:45:39 | 1 second |
| 6 | 30/Jul/2022:22:45:38 | 30/Jul/2022:22:45:38 | 30/Jul/2022:22:45:39 | 1 second |
| 7 | 30/Jul/2022:22:45:38 | 30/Jul/2022:22:45:38 | 30/Jul/2022:22:45:39 | 1 second |
| 8 | 30/Jul/2022:22:45:39 | 30/Jul/2022:22:45:39 | 30/Jul/2022:22:45:39 | 0 second |
| 9 | 30/Jul/2022:22:45:39 | 30/Jul/2022:22:45:39 | 30/Jul/2022:22:45:39 | 0 second |
| 10 | 30/Jul/2022:22:45:39 | 30/Jul/2022:22:45:39 | 30/Jul/2022:22:45:39 | 0 second |
| --- | ---------- | ---------- | ---------- | ---------- |
| 26 | 30/Jul/2022:22:45:42 | 30/Jul/2022:22:45:42 | 30/Jul/2022:22:45:42 | 0 second |
| 27 | 30/Jul/2022:22:45:43 | 30/Jul/2022:22:45:43 | 30/Jul/2022:22:45:43 | 0 second |
| 28 | 30/Jul/2022:22:45:43 | 30/Jul/2022:22:45:43 | 30/Jul/2022:22:45:43 | 0 second |
| 29 | 30/Jul/2022:22:45:43 | 30/Jul/2022:22:45:43 | 30/Jul/2022:22:45:43 | 0 second |
| 30 | 30/Jul/2022:22:45:43 | 30/Jul/2022:22:45:43 | 30/Jul/2022:22:45:43 | 0 second |
| 31 | 30/Jul/2022:22:45:43 | 30/Jul/2022:22:45:43 | 30/Jul/2022:22:45:46 | 3 second |
| | | AVERAGE TIME | | 0.3 second |

Analysis of the notification results of the attack time on the Telegram application can be seen in Table 3. The attack time column is the time when the attacker carried out

the attack. Attack detection time is the time when the TELER detects an attack in the weblog. The received attack information is the time when Telegram received an attack on the web server. Based on the results in Table 3, the average time for 31 attacks is 0.3 seconds, which means 0.3 seconds to send warning notifications to Telegram.

**Scenario 2**

In Scenario 2, Discord became the medium for receiving directory brute force attack information. Table 4 is the result of the Scenario 2.

**Table 4.** Analysis of the Notification Results of the Attack Time on the Discord Application

| No | Attack Time | Attack Detection Time | Receive Attack Information | Receive Attack Information Period |
|---|---|---|---|---|
| 1 | 31/Jul/2022:19:58:14 | 31/Jul/2022:19:58:14 | 31/Jul/2022:19:58:15 | 1 second |
| 2 | 31/Jul/2022:19:58:14 | 31/Jul/2022:19:58:15 | 31/Jul/2022:19:58:15 | 0 second |
| 3 | 31/Jul/2022:19:58:19 | 31/Jul/2022:19:58:18 | 31/Jul/2022:19:58:18 | 0 second |
| 4 | 31/Jul/2022:19:58:22 | 31/Jul/2022:19:58:23 | 31/Jul/2022:19:58:23 | 0 second |
| 5 | 31/Jul/2022:19:58:26 | 31/Jul/2022:19:58:26 | 31/Jul/2022:19:58:26 | 0 second |
| 6 | 31/Jul/2022:19:58:29 | 31/Jul/2022:19:58:29 | 31/Jul/2022:19:58:29 | 0 second |
| 7 | 31/Jul/2022:19:58:32 | 31/Jul/2022:19:58:32 | 31/Jul/2022:19:58:32 | 0 second |
| 8 | 31/Jul/2022:19:58:35 | 31/Jul/2022:19:58:35 | 31/Jul/2022:19:58:35 | 0 second |
| 9 | 31/Jul/2022:19:58:38 | 31/Jul/2022:19:58:38 | 31/Jul/2022:19:58:38 | 0 second |
| 10 | 31/Jul/2022:19:58:41 | 31/Jul/2022:19:58:41 | 31/Jul/2022:19:58:41 | 0 second |
| 11 | 31/Jul/2022:19:58:44 | 31/Jul/2022:19:58:44 | 31/Jul/2022:19:58:44 | 0 second |
| 12 | 31/Jul/2022:19:58:47 | 31/Jul/2022:19:58:47 | 31/Jul/2022:19:58:47 | 0 second |
| 13 | 31/Jul/2022:19:58:50 | 31/Jul/2022:19:58:50 | 31/Jul/2022:19:58:51 | 1 second |
| 14 | 31/Jul/2022:19:58:53 | 31/Jul/2022:19:58:53 | 31/Jul/2022:19:58:53 | 0 second |
| 15 | 31/Jul/2022:19:58:56 | 31/Jul/2022:19:58:56 | 31/Jul/2022:19:58:57 | 1 second |
| --- | --- | --- | --- | --- |
| 28 | 31/Jul/2022:19:59:36 | 31/Jul/2022:19:59:36 | 31/Jul/2022:19:59:36 | 0 second |
| 29 | 31/Jul/2022:19:59:39 | 31/Jul/2022:19:59:39 | 31/Jul/2022:19:59:39 | 0 second |
| 30 | 31/Jul/2022:19:59:42 | 31/Jul/2022:19:59:42 | 31/Jul/2022:19:59:42 | 0 second |
| 31 | 31/Jul/2022:19:59:45 | 31/Jul/2022:19:59:45 | 31/Jul/2022:19:59:46 | 1 second |
| | | AVERAGE TIME | | 0.12 second |

As can be seen in Table 4, the attack time column shows the time when the attacker carried out the attack. The detection time column is when TELER detects an attack on the weblog. The received attack information is the time when Discord received an attack on the web server. Based on the results in Table 4, the average time for 31 attacks is 0.12

seconds, which means 0.123 seconds to send warning notifications to Discord.

**Scenario 3**

In Scenario 3, Slack became the medium for receiving directory brute force attack information. Table 5 is the result of the Scenario 3.

**Table 5.** Analysis of the Notification Results of the Attack Time on the Slack Application

| No | Time Attack | Attack Detection Time | Receive Attack Information | Receive Attack Information Period |
|---|---|---|---|---|
| 1 | 30/Jul/2022:23:49:11 | 30/Jul/2022:23:49:11 | 30/Jul/2022:23:49:12 | 1 second |
| 2 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 0 second |
| 3 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 0 second |
| 4 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 0 second |
| 5 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 0 second |
| 6 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 0 second |
| 7 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 0 second |
| 8 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 0 second |
| 9 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 0 second |
| 10 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 30/Jul/2022:23:49:12 | 0 second |
| --- | --- | --- | --- | --- |
| 26 | 30/Jul/2022:22:45:15 | 30/Jul/2022:22:45:15 | 30/Jul/2022:23:49:15 | 0 second |
| 27 | 30/Jul/2022:22:45:16 | 30/Jul/2022:22:45:16 | 30/Jul/2022:22:45:16 | 0 second |
| 28 | 30/Jul/2022:22:45:16 | 30/Jul/2022:22:45:16 | 30/Jul/2022:22:45:16 | 0 second |
| 29 | 30/Jul/2022:22:45:16 | 30/Jul/2022:22:45:16 | 30/Jul/2022:22:45:16 | 0 second |
| 30 | 30/Jul/2022:22:45:16 | 30/Jul/2022:22:45:16 | 30/Jul/2022:22:45:16 | 0 second |
| 31 | 30/Jul/2022:22:45:16 | 30/Jul/2022:22:45:16 | 30/Jul/2022:22:45:16 | 0 second |
| | | AVERAGE TIME | | 0.03 second |

As can be seen in Table 5, the attack time column shows the time when the attacker carried out the attack. The detection time column is when TELER detects an attack on the weblog. The received attack information is the time when Slack received an attack on the web server. Based on the results in Table 5, the average time for 31 attacks is 0.03 seconds, which means 0.03 seconds to send warning notifications to Slack.

## CONCLUSIONS, RECOMMENDATIONS, AND LIMITATIONS

Based on the experiments concluded in this study, it can be concluded that Slack is the most effective application for receiving directory brute-force attack notifications because it has an average time of 0.03 seconds to receive attack information from web server attacks by using dirsearch. TELER successfully detects attacks well, namely by displaying the type of attack that is in progress, the attacker's IP, the user agent attacker, the time of the attack, as well as the status code sent by the server. The detection results are sent to the application properly with an average delay of less than 1 second. For further research, it is recommended to combine the experiment conducted in this study with fail2ban as an intrusion prevention system. After detecting attacks using TELER,

fail2ban could serve to block attackers so that server security becomes more secure. This study could be beneficial to anticipate cyber attacks within defense and security scope in the future.

**REFERENCES**

Akram, W., & Kumar, R. (2017). A Study on Positive and Negative Effects of Social Media on Society. *International Journal of Computer Sciences and Engineering*, *5*(10), 351–354. https://doi.org/10.26438/ijcse/v5i10.351354

Alfidzar, H., & Zen, B. P. (2022). Implementasi HoneyPy dengan Malicious Traffic Detection System (Maltrail) Menggunakan Analisis Deskriptif guna untuk Mendeteksi Serangan DDOS pada Server. *Journal of Informatics Information System Software Engineering and Applications (INISTA)*, *4*(2), 32–45. https://doi.org/10.20895/inista.v4i2.534

Anggarini, D., Zen, B. P., & Pranata, M. (2022). Security Analysis On Websites Using The Information System Assessment Framework (Issaf) And Open Web Application Security Version 4 (OWASPv4) Using The Penetration Testing Method. *Jurnal Pertahanan*, *8*(3), 2549–9459. https://doi.org/10.33172/jp.v8

BSSN. (2023). Honey Project. Retrieved from https://bssn.go.id/honeynet-project/

CNN Indonesia. (2018). Kemhan Terima 80 Ribu Serangan "Hacker" Tiap Hari. Retrieved from CNN Indoensia website: https://www.cnnindonesia.com/Teknologi/20181107155049-185-344721/kemenhan-terima-80-ribu-serangan-hacker-tiap-hari. Accessed on Desember 01, 2023.

Hidayat, S., Thamrin, S., & Widayatno, R. L. (2022). Russia And Japan War Based On Military Perspective. *Jurnal Pertahanan*, *8*(1), 177–188. http://dx.doi.org/10.33172/jp.v 8i1.1620

Ma, K., Jiang, R., Dong, M., Jia, Y., & Li, A. (2017). Neural Network-based Web Log Analysis for Web Intrusion Detection. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics),*. https://doi.org/10.1007/978-3-319-72395-2_19

Siswanto, D. (2023). TELER. Retrieved from Kita Bisa website: https://github.com/Kitabisa/TELER. Accessed on December 01, 2023.

Tabash, M., Allah, M. A., & Tawfik, B. (2020). Intrusion Detection Model Using Naive Bayes and Deep Learning Technique. *International Arab Journal of Information Technology*, *17*(2), 215–224. https://doi.org/10.34028/iajit/17/2/9

Tedyyana, A., Ghazali, O., & Purbo, O. W. (2021). *TELER Real-time HTTP Intrusion Detection at Website with Nginx Web*. *5*(September), 327–332. https://dx.doi.org/10.30630/joiv.5.3.510

William, P., Choubey, A., Chhabra, G. S., & Bhattacharya, R. (2022). Assessment of Hybrid Cryptographic Algorithm for Secure Sharing of Textual and Pictorial Content. *International Conference on Electronics and Renewable Systems (ICEARS)*. IEEE Xplore. https://doi.org/10.1109/icears53579.2022.9751932

Zen, B. P., Anggi, Z., & Putro, I. N. Y. (2022). Network Security Analysis Simulation at the GCS in the UCAV to support the Indonesian Defense Area. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *6*(5), 824–831. https://doi.org/10.29207/resti.v6i5.4412

Zen, B. P., Gultom, R. A. G., & Reksoprodjo, A. H. S. (2020). Analisis Security Assessment Menggunakan Metode Penetration Testing dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara. *Jurnal Teknologi Penginderaan*, *2*(1), 105–

122. https://jurnalprodi.idu.ac.id/index.php/TP/article/view/574