Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 10, No. 4, November, Pp. 455-464

Post attack mitigation on open journal system services using knowledge understanding assessment defense (KUAD) method

Hero Wintolo*[1,2], Imam Riadi[3], Anton Yudhana[4]
Informatika, Universitas Ahmad Dahlan, Yogyakarta, Indonesia[1]
Informatika, Institut Teknologi Dirgantara Adisutjipto, Yogyakarta, Indonesia[2]
Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta, Indonesia[3]
Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta, Indonesia[4]

Article Info

Keywords:
Mitigation, Attacking, Open Journal System, Knowledge Understanding Assessment Defense

Article history:
Received: March 13, 2025
Accepted: July 01, 2025
Published: November 01, 2025

Cite:
H. Wintolo, I. Riadi, and A. Yudhana, “Post Attack Mitigation on Open Journal System Services using Knowledge Understanding Assessment Defense (KUAD) Method”, *KINETIK*, vol. 10, no. 4, Nov. 2025. https://doi.org/10.22219/kinetik.v10i4.2279

*Corresponding author.
Hero Wintolo
E-mail address:
2437083004@webmail.uad.ac.id

Abstract

This research was conducted to investigate evidence of an attack and to restore data after an attacker compromised an Open Journal System (OJS) service on a computer server. The method used in this research is a new approach developed from the Network Forensic Digital Life Cycle (NFDLC) method. This new method, known as KUAD, has several stages for collecting cyber-attack evidence and restoring it after the Gacor attack has occurred. The stages in the KUAD method include initiation, acquisition, execution, mitigation, and disposition. The novelty of this method, compared to the previous one, lies in the inclusion of the mitigation stage, which aims to restore data or documents after an attack. The tool used to detect the attack and find evidence of the attack is Tripwire, whereas the tools used to restore lost data include crontab, which runs backup commands with rsync in four steps. Tripwire can optimally detect attacks by displaying the number of data entries that were added, deleted, or modified. A total of 15,135 files in .docx, .pdf, and .jpg formats, deleted by the attacker, were successfully restored using this backup technique. The success rate of using this technique for post-cyber attack mitigation reached 100%.

1. Introduction

Security disturbances in computer network environments targeting attacks on end devices, intermediary devices, and even the physical layer of a computer network never cease and always cause significant damage to those impacted by these attacks. One of the consequences of an attack on an end device, such as a computer server used to provide services for writing scientific articles using the OJS application, is one of the most critical issues. The security of the OJS service has now become a particular concern due to the increasing adoption of this system in various academic institutions to support online scientific publication management. Although OJS offers convenience in article management, review processes, and publication, it also harbors significant security risks. Vulnerabilities in server configurations, a lack of reliable file monitoring mechanisms, and the absence of comprehensive post-attack mitigation procedures make OJS a vulnerable target for cyberattacks, including data deletion, infiltration, and file modification by unauthorized parties. This reality shows that many institutions still lack adequate emergency response procedures to recover data after an attack. As a result, many scholarly journals lose important documents, such as author manuscripts, review results, and valuable metadata. Therefore, system administrators and researchers must have mitigation strategies that are not only capable of detecting but also of accurately and swiftly restoring data after an attack. The impact of this attack must be addressed carefully and systematically through a process known as mitigation.

Recent advancements in cybersecurity emphasize the integration of digital forensics and automated mitigation techniques to address increasingly sophisticated cyberattacks on critical online services, including academic publishing platforms like OJS.The mitigation approach that systematically and effectively handles post-attack data recovery for OJS services has yet to be discussed. Common methods, such as NFDLC, focus primarily on forensic investigation processes without addressing data repair and recovery aspects. Furthermore, there has been little research specifically focusing on the implementation of mitigation against cyberattacks on OJS systems, despite the widespread adoption of this platform by academic institutions. This gap serves as the foundation for developing the KUAD method proposed in this study, which not only detects and logs attacks but also restores the affected data with a high success rate. The novelty of this study lies in the integration of a dedicated mitigation phase within the forensic process, absent in prior models like NFDLC, along with the practical application of automated backup techniques using `rsync` and Tripwire to fully restore compromised data in OJS.

Mitigation against insider threats in computer networks requires various techniques or methods, such as behavioral analysis, anomaly detection, and access management, to protect the organization's security from attacks originating from internal users who may potentially abuse their privileges [1]. In addition, mitigation is also important for detecting and reducing the impact of attacks on intermediary devices, such as switches affected by flooding attacks, which can improve the efficiency and security of the NDNoT network by managing timeouts on Pending Interest Tables (PIT), achievable through the Interest Flooding Networking of Things (IfNoT) approach [2]. To address threats in computer networks used by the Internet of Things (IoT), mitigation methods can implement the Recurrent Neural Network (RNN) algorithm, which leverages processed data and extracted features. This approach achieves high accuracy in threat classification on both training and testing datasets [3]. Mitigation carried out post-attack will be effective if preceded by the detection of the object that is the target of the attack.

The detection and mitigation method for ARP spoofing attacks in Software-Defined Networking (SDN) using a Deep Neural Network (DNN) model has demonstrated perfect accuracy, achieving 100% detection accuracy[4]. On the other hand, a systematic literature review of 248 articles on mitigation strategies against phishing attacks emphasizes the importance of considering human user capabilities in the development of mitigation strategies, as solutions that focus solely on technology are insufficient to address the complex challenges of phishing [5]. In the context of DDoS attack mitigation [6], a machine learning-based scheme in ISP networks with SDN architecture has proven to be efficient, with a mitigation success rate of over 98% for TCP-SYN and ICMP attacks, while maintaining the smooth flow of legitimate traffic [7]. The DDoS attack mitigation strategy supported by SDN technology in IoT environments underscores the importance of a collaborative approach and hybrid solutions that integrate blockchain, fog computing, and cloud computing to enhance the effectiveness of mitigation in complex scenarios [8]. Blockchain technology and smart contracts have been utilized to detect and mitigate the impact of DDoS attacks, particularly those based on TCP, achieving a detection success rate exceeding 99% and maintaining very low false positive and false alarm rates [9]. Machine learning-based mitigation techniques, such as Random Forest and K-Nearest Neighbors, are also effective in detecting and mitigating the impact of DDoS attacks in SDN networks by blocking suspicious traffic at the point of attack to maintain network service stability [10].

The use of signature-based methods in Intrusion Detection Systems (IDS) enables the recognition of attack patterns through TCP and UDP protocols, providing accurate detection results via a web-based interface [11]. The implementation of Unified Threat Management (UTM) based on open-source applications, combining Snort as an Intrusion Prevention System (IPS) and Splunk as a Security Information and Event Management (SIEM) system, has proven effective in enhancing threat mitigation and bandwidth efficiency in TCP/IP networks. Blockchain technology, combined with the Advanced Encryption Standard (AES) cryptography, has been applied to enhance the security of digital transactions, such as online pocket money top-ups in school environments, with strong resistance to Cross-Site Scripting (XSS) attacks [12]. The malware cyberattack detection technique using network traffic analysis based on Neural Networks aims to improve malware detection accuracy on IoT devices and smartphones by analyzing 79 features from network traffic data to classify malware into three categories: adware, general malware, and benign applications [13]. A hybrid blockchain-based security model prototype is designed to enhance data security in public organizations, with an effectiveness of 99.50% against cyberattacks through simulations that include a layered security architecture and anomaly detection algorithms to identify and prevent unauthorized access to public databases [14]. In addition, the development of a new attack, called SIP Request-Based Distributed Reflection DoS (SR-DRDoS), which exploits vulnerabilities in the SIP protocol through reflection and IP spoofing techniques, yielded simulation results showing an increase in the CPU load of the SIP server from 0% to 100% within 4 minutes. However, the proposed defense mechanism successfully reduced the CPU load from 71% to 18% within 3 minutes [15].

The Random Port Knocking (RPK) method has proven effective in enhancing network security with the principles of availability, confidentiality, and integrity. It is capable of blocking brute force and port scanning attacks with a 100% blocking success rate [16]. Additionally, implementing a Packet Filtering Firewall at Layer 3 and a Circuit-Level Gateway Firewall at Layer 4 can significantly reduce DDoS attack traffic [17]. Live memory forensics techniques also play a crucial role in mitigating ransomware attacks, particularly those utilizing the Salsa20 encryption algorithm, by enabling the extraction of the encryption key during the execution process, thereby allowing the victim's files to be decrypted without paying the ransom. However, this method still faces challenges when dealing with custom algorithms [18]. In the era of IoT development, ransomware attacks have become a significant and increasingly prevalent threat, as malware spreads more easily and causes substantial losses for both individuals and organizations. Therefore, effective mitigation efforts are crucial to prevent harmful impacts [19]. Mitigation steps are also applied to the e-skimmer threat on e-commerce platforms through the NAISS solution, which utilizes digital signatures to prevent the delivery of malicious content and maintain data integrity [20]. Furthermore, the use of data mining and machine learning has proven to significantly enhance cyber threat mitigation by analyzing patterns and trends from previous incidents, enabling better detection and prediction to strengthen network resilience [21].

The implementation of a deep learning-based Intrusion Detection System (IDS), such as IDSX-Attention, has proven effective in enhancing cyberattack detection through dimensionality reduction and attention mechanisms, thereby improving attack classification accuracy. This is crucial in efforts to mitigate increasingly complex cyber threats [22]. Furthermore, the importance of risk mitigation in online education management systems can also be achieved through the ITIL v3 framework standards, which not only help identify the level of data security but also provide recommendations to improve security operations, thereby reducing the potential for security incidents in the use of the WIOEM system [23]. The threat mitigation strategy for electronic payment systems emphasizes the use of blockchain technology and machine learning to enhance transaction security and prevent data leaks and unauthorized access to user accounts [24]. Meanwhile, mitigation of crypto-jacking attacks can be achieved through the implementation of an Intrusion Detection and Prevention System (IDPS) based on Suricata devices equipped with custom rules, resulting in 100% detection effectiveness, an improvement in recall to 48.94%, and an F-measure of 32.39% [25]. The attack mitigation is carried out using the Open Web Application Security Project (OWASP) method [26], particularly in identifying and addressing vulnerabilities such as Broken Authentication and Sensitive Data Exposure, by providing recommendations for server configuration improvements and regular system updates [27].

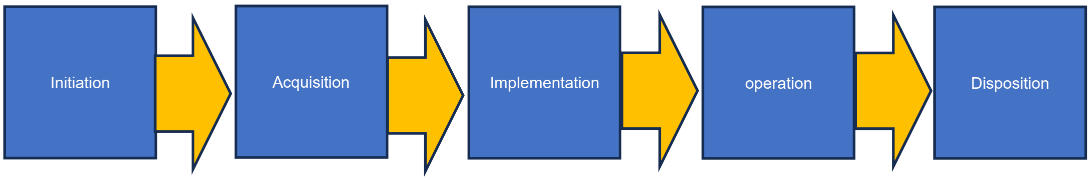


Figure1. NFDLC Method[28]

Various mitigation efforts that have been widely implemented to repair damage after a cyberattack will be applied in the NFDLC method, as shown in Figure 1. The novelty of this method in this research lies in the mitigation performed after the attack. Additionally, the research object on the OJS service and the backup technique used represent innovations in OJS mitigation. This article is worth reading because it offers an innovative post-attack mitigation approach for OJS through the KUAD method. This method builds upon NFDLC and introduces an additional phase focused on systematic data recovery, which has not been widely discussed in other studies. The use of Tripwire to detect file modifications in real-time, combined with an automatic backup technique using `rsync` scheduled with `crontab`, makes this approach unique and proven effective with a high data recovery rate during the mitigation steps. The novelty of the KUAD method, the specific research object on the OJS service, and the modular and responsive backup technique make this article an important contribution to the realm of scientific publication system security. Readers seeking a practical, systematic, and proven approach to managing security incidents on OJS will find great value in this article. Understanding and applying an effective post-attack mitigation strategy, such as the KUAD method introduced in this study, is essential for institutions seeking to safeguard the integrity of their academic publishing systems.

2. Research Method

The method used in this research is an enhancement of the NFDLC Method, which involves configuring, integrating, and adding aspects related to post-cyberattack incident response. This method has not been previously developed or used by other researchers, making it a novel and innovative element of this study. The process, as shown in Figure 2, is named KUAD, which stands for Knowledge Understanding Assessment Defense.

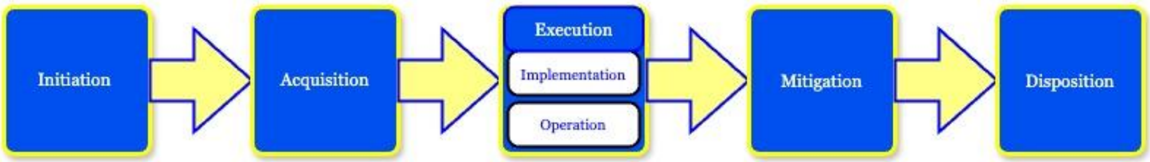


Figure 2. KUAD Method

This method has a sequence for handling cyberattacks, presented as follows:

1. Initiation
   The primary focus of this stage is the initial risk assessment of end devices and intermediary devices in terms of their potential vulnerability to attack. This will greatly assist in making informed decisions about the software and hardware used, as well as their vulnerabilities to potential attacks. At this stage, the input consists of initial system logs, followed by a report from the administrator regarding access disruptions and symptoms such as defaced pages and errors during admin login. The main activities carried out include an initial identification of system anomalies in the OJS, determining the targeted objects, and preparing a forensic investigation plan. The output consists of a forensic planning document, investigation focus areas, and an initial identification that the attack involves defacement and file manipulation.

2. Acquisition
   This stage involves collecting data for the investigation, which requires several software tools. With established standards for the tools used, the evidence obtained can be effectively utilized in subsequent processes. The input on the OJS server includes system and application log files as well as the OJS file directories. The main activities involve forensic backup using Tripwire, copying and securing log files, and performing hashing to maintain the integrity of the evidence. The output consists of copies of the affected OJS data, hash values for integrity verification, and log files that will be used for subsequent analysis and review.
3. Execution
   The implementation stage is the integration of the implementation and operation stages in the NFDLC method. This stage is used to collect data that can later be used as evidence of a crime, ensuring that proper documentation is maintained so it can be utilized without the need to start over. In this stage, every improvement made to address an attack must be carefully recorded. This serves as preparation and anticipation in case the same attack recurs, potentially with the same impact or even more severe damage. The input consists of log files, OJS backup files, configuration files, and previously generated hash results. The primary activities involve analyzing log files to identify suspicious activities (such as unauthorized access and file changes), detecting shell files, and tracking the attacker's IP address, access times, and exploitation methods (potentially through plugin upload vulnerabilities or form submissions). The output includes a forensic analysis report, attack chronology, malicious files, and compromised user accounts.
4. Mitigation
   This stage is used to mitigate the consequences of an attack that results in loss and damage to the targeted objects. In this stage, techniques for handling cyberattacks are also applied, categorized into recovery and restoration efforts. The input consists of execution reports and files that were manipulated or deleted by the attacker. The activities carried out include restoring important OJS files from backups, utilizing tools such as Tripwire for detecting file changes, applying `rsync` for data synchronization from the backup, and removing malicious files from the server. The output includes a fully functional OJS system, restored files in their entirety, and a more secure server configuration.
5. Disposition
   The final stage is the disposition phase, where the documents prepared and created for security purposes and actions to protect the targeted devices are sent to the highest leadership, who is responsible for the institution where the devices were attacked and subsequently mitigated. The input at this stage includes the results of recovery and mitigation, analyzed log files, the attack chronology, and the mitigation steps. The primary activities include preparing a comprehensive forensic report (including findings, perpetrators, methods, and impacts), providing security recommendations, educating system administrators, and archiving digital evidence for legal purposes. The output consists of the final forensic report, recommendations for enhancing OJS security, and a system that is ready for use again.

The development of the KUAD method as an enhancement of NFDLC was carried out through a scientific approach based on critical analysis of the limitations of NFDLC, namely the absence of a mitigation stage for data recovery post-attack. This research not only proposes a new framework but also implements it technically on a real system (OJS service) and conducts a comparative experiment against the previous method.

3. Results and Discussion

3.1 Initiation

The initiation stage, which is the first step in this research, is used to prepare the hardware and software. The composition of the hardware and software used in this research is illustrated in Figure 3. The OJS software is installed on top of the Ubuntu Linux operating system on the server computer. In addition to OJS and the operating system, web server software and database server software must also be installed on this hardware. This stage establishes that the OJS has experienced changes on the main page, and the admin login has been redirected, indicating the exploitation of upload vulnerabilities and file injection.

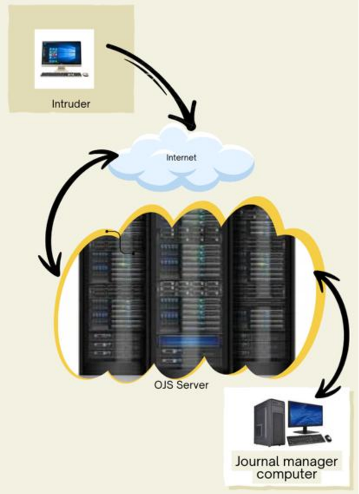


Figure 3. The Hardware Used in this Research

The function of the journal manager's computer is to receive information from monitoring results and execute server security actions. To allow the manager to perform monitoring tasks on OJS, the Tripwire tool must be installed on the server computer. The monitoring and remote control process, known as remote access, should be carried out as close as possible to the server or still within the same network address as the server that the journal manager is responsible for, to manage the journal using OJS and prevent attacks aimed at blocking the journal manager's access to the server computer.

3.2 Acquisition

Research preparation in the initiation stage involves setting up the necessary software, hardware, and internet connection, followed by transitioning to the next stage, which is acquisition. This stage is used to collect data resulting from the attack carried out by hacker tools, with Tripwire being the tool used for this purpose. The wave of attacks that occurred used Gacor file injection techniques targeting all applications on the server, including OJS. As shown in Figure 4, Tripwire, a network security tool, is installed on the server computer alongside other software, although the focus of this research remains solely on OJS.

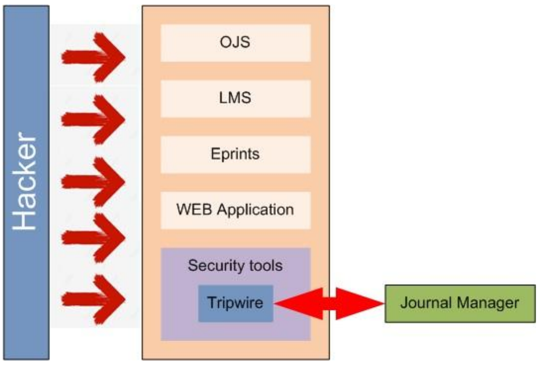


Figure 4. The Composition of the Equipment Used to Collect Data

The source of the attack comes from the hacker, who sends various attacks (indicated by the red arrows) to the system, with OJS being the target of the attack. The server's security system, in the form of security tools, utilizes Tripwire to detect changes in system files that may occur due to suspicious activities resulting from hacker attacks. Monitoring file attribute changes with Tripwire, integrity validation is performed by comparing the SHA-256 hash values of the system files against those of the OJS system files. Based on the checks using hash values to test the data between the conditions before and after the incident, no illegal modifications were found in the data from the acquisition results using Tripwire. The role of the journal manager, who has access, is to monitor and manage Tripwire to detect changes that could potentially harm the system. Tripwire assists the journal manager by displaying data on changes that have occurred in OJS, as discussed in the previous article [28]. The change in the number of documents presented using this tool can be used as digital evidence of an attack on OJS. At this stage, the files `index.php` and `config.inc.php` are suspected to be the objects that have been modified or replaced with files containing a shell or deface script during the Gacor attack process.

3.3 Execution

This stage is used to execute the preparations and setup of the equipment from the previous stages. The first step is the configuration process of Tripwire, as shown in Figure 5. This configuration includes specifying the target directories to be scanned, the scan frequency, the status of directories (whether added, modified, or removed), and the scan results in the form of messages that will be sent via email.

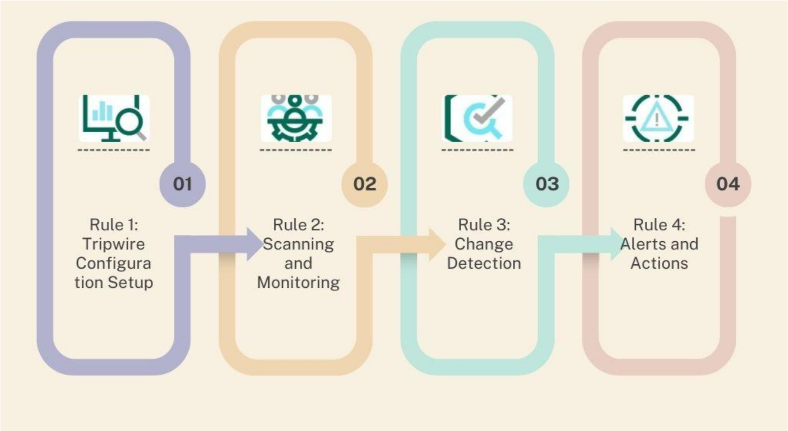

01
Rule 1: Tripwire Configura tion Setup
02
Rule 2: Scanning and Monitoring
03
Rule 3: Change Detection
04
Rule 4: Alerts and Actions

Figure 5. The Sequence for Setting up Tripwire

The configuration process is carried out by editing the Tripwire Policy File with a text editor on the journal manager's computer. Several source codes need to be added to introduce new rules in the `/etc/tripwire/twpol.txt` file, including the following:

```
1. (
2.    rulename = "WebServer",
3.    severity= $(SIG_HI),
4.    emailto = 2437083004@webmail.uad.ac.id
5.   ) {
6.          /var/www/html/OJS/         -> $(SEC_CRIT);
7.   }
8. /usr/sbin/tripwire-- check -c tw.cfg | mail s "Tripwire report for `uname-n`,
   errors found" root@ctfdiary
```

The results of the scan performed using Tripwire will be sent to the email address specified in source code item number 4. The journal manager who receives the email must immediately process and read the scan data using this tool by typing the following command: `tripwire -m c-s -c /etc/tripwire/tw.cfg`, which displays information on the number of files that were added, modified, and deleted. The scan data are validated with the Apache logs, which identify unauthorized activity originating from an IP address that made an HTTP POST request to the endpoint `/plugins/generic/xyz/upload.php`. The logs also show repeated login attempts to the administrator account at the time of the attack, which does not align with the system admin's work schedule. This activity suggests a successful brute force attack or exploitation of the upload vulnerability.

3.4 Mitigation

The results of the scan, using Tripwire tools in the execution phase, are used to repair the damage caused by the attackers. The repair, in the form of restoration during the mitigation phase, uses a backup technique with `rsync` [29], as shown in Figure 6. This technique is carried out in four independent steps, each of which is unrelated to the others. The backup technique is a term coined by the researcher, where the existing backup is restored to recover lost data after the attack, thereby bringing OJS back to normal. In steps two through four, the backup script is written into a file scheduled using `crontab`, while the first step is executed directly based on specific conditions. For example, if step two does not execute properly or in the event of a force majeure, a decision is made to proceed immediately with the backup process.

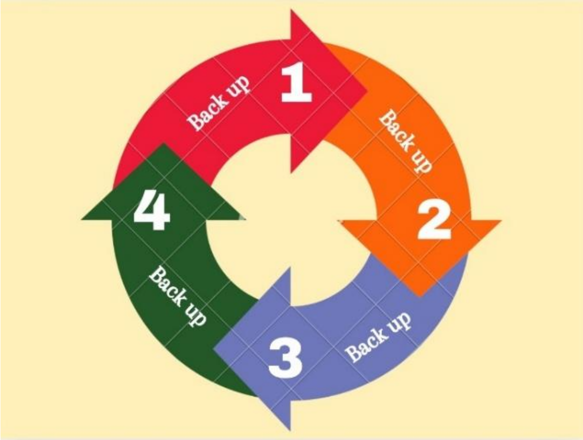


Figure 6. The Mitigation Process Using the Backup Technique

The four steps in the backup technique used in the mitigation stage to restore lost data or documents after an attack on OJS are as follows:

1. Manual: This step is performed by entering the command `rsync—rt /var/www/ user@10.10.10.10:/home/directory_name/ directory_name/—-omit-dir-times`, which is executed directly from the journal manager computer. This step is neither performed routinely nor scheduled; it is executed only as needed in urgent situations.
2. When a new file is added, the file containing the source code `rsync -rt /var/www/ user@10.10.10.10:/home/directory_name/ directory_name/ --ignore-existing --omit-dir-times` is scheduled in `crontab` for execution at regular intervals. However, this process does not burden the server, as it only runs when a new file is added.
3. Every 2 minutes (Periodic Execution), a scheduled task using `crontab` runs to execute the source code `/2 * * * * sudo rsync -rt /var/www/ user@10.10.10.10:/home/directory_name/ directory_name --ignore-existing --omit-dir-times`. This step is essentially the same as the second step, with the key difference that it is executed at a fixed 2-minute interval.
4. Every day at 22:00, a scheduled `crontab` task executes the source code, which is almost identical to the first step, with the key difference being its execution time. The task runs daily at 22:00 using the command: `0 22 * * * sudo rsync—rt/var/www/ user@10.10.10.10:/home/directory_name/ directory_name—— omit-dir-times`.

Restoring data from a backup is carried out by reversing the commands in the source code in four steps. For example, the command: `0 22 * * * sudo rsync -rt /home/directory_name/directory_name user@10.10.10.10:/var/www/tikstta --omit-dir-times` transfer data from `/home/directory_name/directory_name` to `/var/www/`, ensuring that any lost data or documents in the OJS directory are restored to their pre-attack state. The backup data restoration to the server computer, containing several applications as shown in Table 1, demonstrates that this mitigation approach for managing OJS services is effective. This aligns with the research objective of restoring data and documents after an attack on the OJS research subject.

Table 1. Mitigation Results

No	The name of the journal in OJS	Number of lost documents	Number of returned documents
1	Angkasa	2183	2183
2	Cakrawala	614	614
3	Kacanegara	7208	7208
4	Avitec	2412	2412
5	Compiler	1458	1458
6	Jumantara	470	470
7	Vortex	488	488

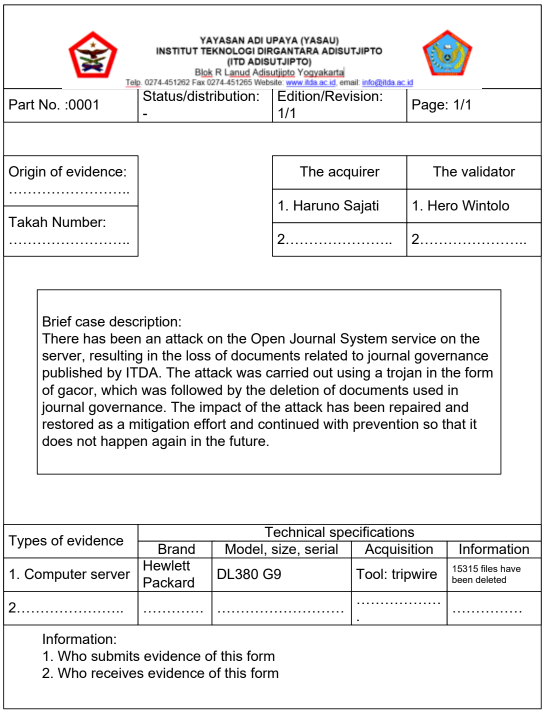
The attack affected seven journals in the OJS application and was successfully mitigated. The lost documents that were successfully restored all consisted of uploaded documents, revisions, and publications, which were in the form of DOC/X and PDF files. The results presented in Equation 1, derived from the mitigation process, are used as parameters for the quantitative evaluation of sensitivity using the Detection Rate (DR). The synchronization process of the backup results is used to measure the effectiveness of the mitigation efforts on the OJS service, expressed as a percentage. The recovery process not only ensured the recovery of 100% of the lost documents but also demonstrated the practicality of the `rsync`-based backup approach in real operational environments, validating its reliability under active attack conditions.

$$DR = \frac{\text{Number of documents returned}}{\text{Number of documents lost}} x\ 100\% = \frac{15315}{15315} x100 = 100\% \tag{1}$$

The data was successfully recovered after the attack through the mitigation process, utilizing the backup technique, which was carried out in four steps. Each step is independent of the others in terms of execution intensity. The amount of data that was successfully recovered does not depend on whether the backup step was executed through `crontab` or manually. The results of the mitigation in this research show that the backup-based approach using the `rsync` technique, both automatically and manually, can restore all documents lost due to the attack. Unlike the entropy detection and honeypot integration approach [30], this research focuses on comprehensive data recovery post-attack, which has proven to be effective in restoring OJS. To validate the effectiveness of the KUAD method, the mitigation results were compared with those of previous approaches, such as NFDLC, which lacks an explicit phase for data recovery. In NFDLC, the process ends at reporting and documentation, thus not providing a technical mechanism to restore documents deleted due to the attack. In contrast, the KUAD method incorporates a more comprehensive mitigation phase, utilizing an automated backup technique based on `rsync` and `crontab`, which enables real-time data recovery. In the context of the OJS service, the KUAD method demonstrates superiority because it not only detects attacks but also restores the impacted data, achieving a 100% success rate, as evidenced by the recovery of all documents in the seven analyzed journals.

3.5 Disposition

The final stage of the KUAD method is reporting to the leadership regarding the success in handling the attack on OJS. The form and format of the report can be adjusted according to the institution targeted by the attackers. The most important elements that must be included in the report document are information about the occurrence of the attack, evidence of the attack, and confirmation that the impact has been mitigated by restoring all lost data.



YAYASAN ADI UPAYA (YASAU)
INSTITUT TEKNOLOGI DIRGANTARA ADISUTJIPTO
(ITD ADISUTJIPTO)
Blok R Lanud Adisutjipto Yogyakarta
Telp. 0274-451262 Fax 0274-451265 Website: www.itda.ac.id, email: info@itda.ac.id

Part No. :0001	Status/distribution: -	Edition/Revision: 1/1	Page: 1/1

Origin of evidence:
……………………..

Takah Number:
……………………..

The acquirer	The validator
1. Haruno Sajati	1. Hero Wintolo
2…………………..	2…………………..

Brief case description:
There has been an attack on the Open Journal System service on the server, resulting in the loss of documents related to journal governance published by ITDA. The attack was carried out using a trojan in the form of gacor, which was followed by the deletion of documents used in journal governance. The impact of the attack has been repaired and restored as a mitigation effort and continued with prevention so that it does not happen again in the future.

Types of evidence	Technical specifications			
	Brand	Model, size, serial	Acquisition	Information
1. Computer server	Hewlett Packard	DL380 G9	Tool: tripwire	15315 files have been deleted
2……………………	…………	………………………	……………… .	……………

Information:
1. Who submits evidence of this form
2. Who receives evidence of this form

Figure 7. Letter Disposition to the Supervisor

Figure 7 shows one form of document used in the disposition stage and includes the main attachment of the digital forensic report, which is not displayed in this article. The documentation of the attack on OJS is thoroughly compiled, including the attacker's IP address, malicious files, and the vulnerabilities exploited. The administrator also receives guidelines for future prevention. This document will be very useful for the leadership to conduct an evaluation or even take further action by reporting the losses from the attack to the authorities responsible for handling cybersecurity in the country. The validity of the KUAD method is reinforced by quantitative results, with a 100% data recovery success rate, as well as its ability to detect and restore important documents deleted by hackers. By incorporating a mitigation phase and utilizing tools such as Tripwire and `rsync`, KUAD addresses the gaps in NFDLC, enhancing its ability to handle cyber incidents.

4. Contribution

The research conducted on the OJS platform, using the KUAD method and tools like Tripwire and `rsync` in dealing with Trojan attacks like Gacor, makes a positive contribution. KUAD is an enhancement of the NFDLC method, adding an important mitigation phase that was previously absent in digital forensics approaches. This enriches the academic discourse in the fields of digital forensics and information system security, particularly in the context of post-attack incident response. The KUAD method is specifically designed to address attacks on OJS services, offering a novel approach to mitigation in the domain of web-based scholarly journal management. KUAD can serve as a reference for further research on expanding mitigation methods to other online publishing systems or services. This research contributes to the knowledge of designing modular backup techniques based on `rsync` and `crontab`, which are integrated into a digital forensics-based mitigation system.

Practically, KUAD has proven to restore 100% of the lost data from the 7 OJS journals that were attacked, making it directly applicable by network administrators managing scholarly journals in real-world scenarios. The article presents a comprehensive technical implementation, from Tripwire configuration and backup scheduling using `crontab` to data recovery, which can serve as a practical guide for IT security practitioners, system administrators, or journal system managers. KUAD functions as both a strategic and technical framework for educational institutions and publishers to enhance the resilience of their systems against cyber incidents, without relying on expensive commercial solutions.

5. Conclusion

The KUAD method used in this research has been successfully implemented to mitigate attacks on a targeted computer server, which hosts the OJS application for journal management. A total of 7 journals in OJS were attacked, resulting in the loss of data in the form of DOC/X and PDF files. By applying the KUAD method, which includes stages in digital forensics and adds a mitigation phase, the affected OJS journals were able to recover from the attack. All stages of this method have been proven applicable for attack mitigation. Deleted documents were recovered using a four-step tiered backup technique. A total of 15,315 lost documents in doc/x, PDF, and JPG formats within OJS were detected using Tripwire software. These lost documents were successfully restored using the `rsync` backup technique, achieving a 100% success rate and proving its reliability for mitigation purposes. Although the KUAD method has proven effective in recovering data after an attack on the OJS service, with a 100% success rate, several limitations need to be critically addressed. First, the effectiveness of this method heavily depends on the correct initial configuration and the consistency of the backup process execution, which can be challenging in institutions with limited technical resources. Second, this method has not been tested in more complex cyberattack scenarios, such as ransomware that encrypts files or zero-day attacks; therefore, its applicability remains limited to certain types of attacks, such as data deletion. For future development, the KUAD method can be expanded by integrating encryption mechanisms and machine learning-based detection to handle more sophisticated and dynamic attack types. Additionally, implementing a real-time notification system based on a visual dashboard and automated damage assessment will enhance the responsiveness of the mitigation system. Further testing on a multi-server scale and cloud integration is also an important research opportunity to evaluate the scalability and adaptability of the KUAD method across different digital infrastructures.

References

[1] U. Inayat, M. Farzan, S. Mahmood, M. F. Zia, S. Hussain, and F. Pallonetto, "Insider threat mitigation: Systematic literature review," *Ain Shams Engineering Journal*, 2024. https://doi.org/10.1016/j.asej.2024.103068

[2] S. Bilgili, A. K. Demir, and S. Alam, "IfNot: An approach towards mitigating interest flooding attacks in Named Data Networking of Things," *Internet of Things (Netherlands)*, vol. 25, Apr. 2024. https://doi.org/10.1016/j.iot.2024.101076

[3] S. Yadav, H. Hashmi, D. Vekariya, Z. A. K. N, and V. F. J, "Mitigation of attacks via improved network security in IOT network environment using RNN," *Measurement: Sensors*, vol. 32, p. 101046, Apr. 2024. https://doi.org/10.1016/j.measen.2024.101046

[4] V. Hnamte and J. Hussain, "Enhancing security in Software-Defined Networks: An approach to efficient ARP spoofing attacks detection and mitigation," *Telematics and Informatics Reports*, vol. 14, Jun. 2024. https://doi.org/10.1016/j.teler.2024.100129

[5] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, "Mitigation strategies against the phishing attacks: A systematic literature review," Sep. 01, 2023, *Elsevier Ltd*. https://doi.org/10.1016/j.cose.2023.103387

[6] I. F. Kilwalaga, F. D. S. Sumadi, and S. Syaifuddin, “SDN-Honeypot Integration for DDoS Detection Scheme Using Entropy,” *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, pp. 187–194, Jul. 2020. https://doi.org/10.22219/kinetik.v5i3.1058

[7] N. N. Tuan, P. H. Hung, N. D. Nghia, N. Van Tho, T. Van Phan, and N. H. Thanh, "A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN," *Electronics (Switzerland)*, vol. 9, no. 3, Mar. 2020. https://doi.org/10.3390/electronics9030413

[8] F. S. Dantas Silva, E. Silva, E. P. Neto, M. Lemos, A. J. Venancio Neto, and F. Esposito, "A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios," Jun. 01, 2020, *MDPI AG*. https://doi.org/10.3390/s20113078

[9] A. A. Abdullah and S. A. Hussein, "Detection and Mitigation of Distribution Denial of Service Attack Based on Blockchain Concept," *Ingenierie des Systemes d'Information*, vol. 29, no. 3, pp. 1043–1049, Jun. 2024. https://doi.org/10.18280/isi.290322

[10] M. A. Mohsin and A. H. Hamad, "Performance Evaluation of SDN DDoS Attack Detection and Mitigation Based Random Forest and K-Nearest Neighbors Machine Learning Algorithms," *Revue d'Intelligence Artificielle*, vol. 36, no. 2, pp. 233–240, Apr. 2022. https://doi.org/10.18280/ria.360207

[11] H. Setiawan, M. Agus Munandar, and L. W. Astuti, “Penggunaan Metode Signatured Based dalam Pengenalan Pola Serangan di Jaringan Komputer,” *JTIIK*, vol. 8, no. 3, pp. 517–524, 2021. https://doi.org/10.25126/jtiik.2021834200

[12] A. Fadlil, I. Riadi, and A. Nugrahantoro, “Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology,” *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, vol. 11, no. 3, p. 155, Dec. 2020. https://doi.org/10.24843/lkjiti.2020.v11.i03.p04

[13] V. Jeremias Lewi Engel, E. Joshua, and M. Maoeretz Engel, "Detection of Cyber Malware Attack Based on Network Traffic Features Using Neural Network," *Khazanah Informatika*, vol. 6, no. 1, 2020. https://doi.org/10.23917/khif.v6i1.8869

[14] S. M. Toapanta, O. A. Escalante Quimis, L. E. Mafla Gallegos, and M. R. Maciel Arellano, "Analysis for the evaluation and security management of a database in a public organization to mitigate cyber attacks," *IEEE Access*, vol. 8, pp. 169367–169384, 2020. https://doi.org/10.1109/ACCESS.2020.3022746

[15] I. Melih Tas, B. G. Unsalver, and S. Baktir, "A Novel SIP-Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism," *IEEE Access*, vol. 8, pp. 112574–112584, 2020. https://doi.org/10.1109/ACCESS.2020.3001688

[16] T. Ernawati, Idham Kholid, Dahlan, and D. Rohmayani, "Case Study in Network Security System Using Random Port Knocking Method on The Principles of Availability, Confidentiality and Integrity," *Jurnal Online Informatika*, vol. 9, no. 1, pp. 41–51, Apr. 2024. https://doi.org/10.15575/join.v9i1.1254

[17] A. Yudhana, I. Riadi, and S. Suharti, "Network Forensics Against Volumetric-Based Distributed Denial of Service Attacks on Cloud and the Edge Computing," *International Journal of Safety and Security Engineering*, vol. 12, no. 5, pp. 577–588, Nov. 2022. https://doi.org/10.18280/ijsse.120505

[18] L. Fernandez de Loaysa Babiano, R. Macfarlane, and S. R. Davies, "Evaluation of live forensic techniques, towards Salsa20-Based cryptographic ransomware mitigation," *Forensic Science International: Digital Investigation*, vol. 46, Sep. 2023. https://doi.org/10.1016/j.fsidi.2023.301572

[19] M. Humayun, N. Z. Jhanjhi, A. Alsayat, and V. Ponnusamy, "Internet of things and ransomware: Evolution, mitigation and prevention," Mar. 01, 2021, *Elsevier B.V.* https://doi.org/10.1016/j.eij.2020.05.003

[20] A. C. Rus, M. El-Hajj, and D. K. Sarmah, "NAISS: A reverse proxy approach to mitigate MageCart's e-skimmers in e-commerce," *Comput Secur*, vol. 140, May 2024. https://doi.org/10.1016/j.cose.2024.103797

[21] N. Samia, S. Saha, and A. Haque, "Predicting and mitigating cyber threats through data mining and machine learning," *Comput Commun*, vol. 228, Dec. 2024. https://doi.org/10.1016/j.comcom.2024.107949

[22] H. Hanafi, A. Pranolo, Y. Mao, T. Hariguna, L. Hernandez, and N. F. Kurniawan, "IDSX-Attention: Intrusion detection system (IDS) based hybrid MADE-SDAE and LSTM-Attention mechanism," *International Journal of Advances in Intelligent Informatics*, vol. 9, no. 1, pp. 121–135, Mar. 2023. https://doi.org/10.26555/ijain.v9i1.942

[23] M. C. Pontoan, J. I. SIhotang, and E. Lompoliu, "Information Security Analysis of Online Education Management System using Information Technology Infrastructure Library Version 3," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 22, no. 2, pp. 207–216, Mar. 2023. https://doi.org/10.30812/matrik.v22i2.2474

[24] Amelia Citra Dewi, Erik Iman Heri Ujianto, and R. Rianto, “Electronic Payment Threats and Security: A Systematic Literature Review,” *Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)*, vol. 13, no. 2, pp. 301–315, Jul. 2024. https://doi.org/10.23887/janapati.v13i2.76635

[25] F. Raditya and J. Sidabutar, “Analisis Rules Intrusion Detection Prevention System (IDPS) Suricata untuk Mendeteksi dan Menangkal Aktivitas Crypto Mining pada Jaringan,” *JEPIN*, vol. 8, no. 2, 2022. https://doi.org/10.26418/jp.v8i2.56194

[26] Y. Indrianingsih, A. G. Pamungkas, H. Wintolo, H. Sajati, Gunawan, and D. Nugraheny, "Descriptive Analysis of Web Security Vulnerabilities at Airport Servers Using The Open Web Application Security Project Security Standard," in *2023 International Conference on Electrical and Information Technology (IEIT)*, 2023, pp. 6–11. https://doi.org/10.1109/IEIT59852.2023.10335586

[27] M. I. A. Elfatiha, I. R. Riadi, and R. U. Umar, "Security Analysis of Web-Based Academic Information System using OWASP Framework," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, Aug. 2024. https://doi.org/10.22219/kinetik.v9i4.2015

[28] H. Wintolo, I. Riadi, and A. Yudhana, “Analisis Deteksi Penyusup pada Layanan Open Journal System Menggunakan Metode Network Forensic Development Life Cycle,” *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 8, no. 1, pp. 133–144, 2025, Accessed: Apr. 15, 2025. https://doi.org/10.36080/skanika.v8i1.3284

[29] C. Liu, "Design and Implementation of Graduate Student Enrollment Management Information System Based on Rsync Algorithm," in *Cyber Security Intelligence and Analytics*, S. and L.-G. O. and Z. X. and C. N. D. W. and A. R. N. H. Xu Zheng and Alrabaee, Ed., Cham: Springer International Publishing, 2022, pp. 617–625. https://doi.org/10.1007/978-3-030-96908-0_77

[30] I. F. Kilwalaga, F. D. S. Sumadi, and S. Syaifuddin, “SDN-Honeypot Integration for DDoS Detection Scheme Using Entropy,” *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, pp. 187–194, Jul. 2020. https://doi.org/10.22219/kinetik.v5i3.1058