Detecting Distributed Denial-of-Service (DDoS) Attacks through the Log Consolidation Processing (LCP) Framework

Mohammad Adib Khairuddin a,*, Mohd Rizal Mohd Isa a, Mohd Afizi Mohd Shukran a, Mohd Nazri Ismail a, b, Kamaruzaman Maskat a

a Computer Science Dept., Universiti Pertahanan Nasional Malaysia, Kem Perdana Sungai Besi, Kuala Lumpur, Malaysia
b Cyber Security & Digital Industrial Revolution Centre, Universiti Pertahanan Nasional Malaysia, Malaysia

Corresponding author: *adib@upnm.edu.my

Abstract — One major problem commonly faced by organizations is a network attack especially if the network is vulnerable due to poor security policies. Network security is vital in protecting not only the infrastructure but most importantly, the data that moves around the network and is stored within the organization. Ensuring a secure network requires a complex combination of hardware including both network and security devices, specialized applications such as web filtering and log management, and a group of well-trained network administrators and highly skilled analysts. This paper aims to present an alternative to the current log management solution. A hindrance to the current log management solution is the difficulty in amalgamating and correlating a vast number of logs with different formats and variables. This paper uses a novel framework called Log Consolidation Processing (LCP) based on the System Information Event Management (SIEM) technology, to monitor the behavior and the fitness of a network. LCP provides a flexible and complete solution to collect, correlate, and analyze logs from multiple devices as well as applications. An experiment testing the effectiveness of LCP in detecting DDoS attacks in a campus network environment was conducted, demonstrating a highly successful rate of detection. Besides threat detection and avoidance through log monitoring and analysis, other benefits of implementing the LCP framework are also included. This paper concludes by mentioning suggested enhancements for the LCP framework.

Keywords — Log consolidation processing; LCP framework; SIEM; DDoS; campus network; log monitoring solution.

I. INTRODUCTION

Horn stated that campus networks are small, local networks dedicated to a set geographical area that covers anywhere from a few hundred square meters indoors to a few square kilometers outdoors [1]. Usage is restricted to people or devices affiliated with the campus area, which adds a level of security and control. Even though the networking area is limited and confined, the traffic is not, and the communication is not static. The network experiences constant changes and growth parallel with the organization’s expansion. This creates a need to install multiple network devices from a simple hub to the much-advanced network security hardware. Alarmingly, it is reported that 50% of all cyberattacks hit small companies [2] with a network setup quite like a campus network.

Nowadays, with the demand for continuous access and stable connectivity, the management of a campus network requires a solution that can identify, analyze, correlate, normalize, and secure logs from multiple data sources in the campus network. For this paper, we proposed the use of a novel SIEM-based framework [3] called Log Consolidation Processing or LCP [4] as the solution to manage campus network logs and monitor network attacks.

A distributed denial-of-service (DDoS) attack is an example of a cyber threat that attacks an organization through the network. The nuisance of DDoS is quite rampant, with many reported cases [5], [6] resulting in quite a large sum of monetary loss. DDoS works when the attacker (or a group of attackers) floods a server with internet traffic to prevent users from accessing connected online services and sites [7]. According to Mishra et al. [8], the network is saturated to the extent that the victim can entertain no other request, and the intensity of the attacks mainly depends on the number of zombie machines used.

This paper is divided into several sections. In the Materials and Method section, we generally describe the components and workings of the Log Consolidation Processing (LCP)
framework and highlight the implementation of LCP in a virtual environment of a typical campus network. The Results and Discussion section exhibits one example of a simulated case study involving a DDOS attack successfully detected using the LCP framework. In contrast, the Conclusion section calls attention to the benefits and limitations of the LCP framework and some suggestions for further enhancement.

II. MATERIALS AND METHOD

A. Log Consolidation Processing Framework

The proposed network behavior monitoring solution, the Log Consolidation Processing (LCP) framework, comprises three components: log management, log analysis, and event management. Each of these components has been discussed in great detail in another paper [4]. Once the scope of monitoring has been confirmed and finalized, the LCP framework starts by acquiring logs from all related network devices (such as routers, switches, and firewalls). This acquisition process would also involve collecting other logs, such as event logs and syslogs, from all related application, web, and database servers. This process falls under the first LCP component, Log Management.

Next, the framework requires that the collected raw data be normalized. Logs must be aggregated, classified, and correlated to provide context for the event. The selected data mining method, association analysis, allows a more comprehensive and filtered analysis. This process reflects the second component of LCP, Log Analysis.

The final component of the LCP framework, Event Management, encompasses two main processes. The reporting, alerting, and monitoring process equips the user or an organization to have a specific, focused, real-time monitoring requirement. Dashboard, forms, and integration provide the user or an organization with interactive and visual reports from the analysis of logs, integrated from all the nodes related to the event.

LCP framework is suitable for organizations as an all-in-one approach to ensuring security. Typically, an organization utilizes numerous safety standards for detecting malicious network behaviors. Still, reports are also generated from multiple devices with dissimilar formats and variables, thus creating inconsistencies and false alarms. LCP framework aims to minimize this error. Fig. 1 presents a detailed overview of the LCP framework and the possible tools assigned to each process.

B. Campus Network

A complete campus network is one of the most critical functions in a campus environment. The network environment must fit the requirements of a campus network. The campus network is not static. It must constantly change and grow, and the evolution is often very different from other parts of the infrastructure. Thus, a campus network environment requires a next-generation solution that provides all functions to identify, analyze, correlate, normalize, and secure logs from multiple data sources in the campus network. LCP framework is the perfect tool for this challenge. Fig. 2 illustrates the network diagram of a virtual campus network called UPNMNet. The diagram contains the position and connectivity of related routers, firewalls, servers, and switches. Using a simulated distributed denial of services or DDoS attack targeting the endpoint user environment in the UPNMNet, the next section will reveal the workings and benefits of using the LCP framework.
Fig. 2  UPNMNet network diagram

Fig. 3  Example of an AlienVault asset report
C. Simulation Requirements

For this case study of simulating a DDoS attack targeting the UPNMNet endpoint user environment, the experiment uses three main tools, also mentioned in Fig. 1. These tools are Alien Vault, Sangfor Next Generation Firewall (NGFW), and Web Application Firewall (WAF). AlienVault is used as a log collection agent. Fig. 3 is the screenshot of the AlienVault asset report indicating the existence of a collection agent installed in Sangfor NGFW and other nodes. Sangfor Next Generation Firewall (NGFW) detects malicious activities and server hacking attempts. NGFW faces the Internet as pictured in Fig. 2. Note the existence of two NGFW for redundancy purposes. One of the firewalls will act as the primary or master while the other acts as the slave or backup. Web Application Firewall (WAF) security and audit logs. WAF is also a firewall that mainly safeguards the server segment or server farm.

III. RESULTS AND DISCUSSION

A. Sangfor NGFW (NGFW)

The result of experimenting on the UPNMNet endpoint user environment to catch potential DDoS attacks reveals the efficiency of using NGFW to detect malicious activities and hacking on the server successfully. Moreover, a DHCP server is also used to locate the user by correlating the IP address with its tagged MAC address. Upon running the NGFW, the firewall will indicate the number of affected users, as shown in Fig. 4. Drilling down the analysis, samples are collected from two affected users based on their distinct IP addresses.

Fig. 4 List of the affected users as detected by NGFW

Fig. 5 lists the attack events pertaining to one of the sampled users. For the sake of this paper, the selected user IP address is 172.200.1.196. Fig. 6 shows a more detailed visualized diagram of the attacks on the selected user. This diagram includes top attacks with outbound connection information.
To accurately match the selected user IP address to its tagged MAC address, this experiment uses an Efficient IP Appliance Server for LAN clients or a DHCP Windows Server for Wireless LAN clients. Fig. 7 identifies the selected user with its matching MAC address using the Efficient IP Appliance Server method. Besides identifying affected users, NGFW can also dispense other vital information, such as the timeline of the attack and the attack type, as shown in Fig. 8.
B. WAF Logs

Logs are vital to the working of the LCP framework. Although the logs collected and transmitted using the AlienVault agent are in various standard formats, they will be natively or manually parsed and correlated. The raw data set should be reduced to the event format of the log by linking from one attribute of the source, which is assigned to an attribute of the event log set [9]. In this experiment, WAF, being the gateway to the server farm, provides three necessary logs to LCP for further analysis. The logs are security, audit, and access logs.

Security logs are records of attack and information leak events [10] occurring within the university’s systems and networks. A security log captures information associated with cybersecurity-related events. In this experiment, the security logs were configured to capture potential attacks on a webserver called mycampus.upnm.edu.my, located on the server farm. Fig. 9 captures detailed information regarding one of the attacks.
According to NIST [11], an audit log is a chronological record of system activities, including records of system accesses and operations performed in a given period. Fig. 10 shows the recorded activities in the server farm, tracked over a specific period and time. The pop-up window in the figure captures detailed information on one of the activities.

Zagan and Danubianu [12] stated that access log files are text files containing essential data about server activities, client requests addressed to a server, server responses, etc. Zola [13] reiterates that notion by indicating that an access log is a list of all requests for individual files, such as Hypertext Markup Language files, their embedded graphic images, and other associated files that get transmitted. Fig. 11 paints a complete overview of users accessing the web servers located on the server farm, captured over a specific period and time. The log contains information on the access date and time, the application used, service details with version number, hostname, URL, and client and server IP address with the accompanying connection port number.
Using these three logs (security, audit, and access) collected from WAF, LCP generated a complete analysis of the attacks. Fig. 12 and Fig. 13 show the result of the study. The figures illustrate the number of request validation attacks, one example of a DDoS attack. They recorded and tracked requests totaling up to 754 attacks. The analysis also includes the types of request validation attacks and the date and time of the attacks.
IV. CONCLUSION

The results of the experiment manifest several benefits of the LCP framework. These benefits are,

A. Comprehensive Solution

LCP framework moves away from a single-point solution to a comprehensive system that allows organizations to optimize their security-related functions, such as collecting and managing critical network assets and these asset logs. According to AlSabbagh and Kowalski [14], asset values, if configured correctly, typically highlight the criticality of each asset, thus increasing the success rate of an organization’s business processes. LCP could help identify information security threats and take necessary measures. In addition, LCP can also contribute to the ongoing information security risk management processes and methods [15].

B. Assist Policy and Regulatory Obligations

LCP framework could assist companies and institutions to optimize the execution of processes to support local government policy and regulatory compliance obligations such as the Malaysian Public Sector Cyber Security Framework (RAKKSSA) [16] or the Securities Commission Malaysia Guidelines on Technology Risk Management (SC-GL/2-2023) [17] or international standards such as the ISO/IEC 27001 [18]. It can monitor real-time events and large amounts of long-term data to detect abnormal usage patterns and alert the organization when needed. The sensors (AlienVault) that collect, aggregate, correlate, and analyze audit log data from monitoring entities should be thoroughly evaluated to ensure that the LCP solution can effectively detect the number of significant attacks and generate the least number of false events and alerts.

C. Mitigate Compliance Issues

Compliance policies protect an enterprise’s information system and related resources from internal or external cyber attackers in cybersecurity. Failure to comply with already set cybersecurity regulations could subject their assets, information systems, and data in cyberspace to massive losses accrued due to penalties, litigation of cyberattack issues, and loss of reliability of their services, which could impact their performances and competitiveness [19].

The deployment of the LCP framework contributes to meeting compliance obligations and helps mitigate any non-compliance issues. The report generated by the LCP (as displayed in the figures) presents detailed and focused information that is suitable not only for technical-oriented employees but also appeals to middle and top management. Based on the listed benefits, it is also possible to implement the LCP framework in other environments, such as Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems [20], smart campus [21], [22], power plant [23] and IoT-based platforms [24], [25].

Nevertheless, more attention is needed to policy-oriented automatic response functions close to every security administrator's ultimate dream. There are expected to be more predefined template rules and visual reports as managers become more involved, and compliance continues to be the driving factor. Karlzén [26] stated that as storage prices decrease and processing performance increases, the speed of data reduction will gradually decrease. However, this
situation is unclear as more products are being installed in the network. The rise of installed equipment in most environments will force the LCP solution to adapt by minimizing the analysis duration while keeping a low false alarm rate. Machine language is one area that can be applied here as it has been shown to excel in other unrelated fields such as social media analytics [27], [28], the COVID-19 pandemic [29], [30], and flood prediction [31]. Finally, with increasing attention to user tracking, the LCP may include identity and access management capabilities, which in this case, will be closer to a complete cyber security monitoring solution.

REFERENCES

[1] U. Horn, “What is a 5G Campus Network?,” Web. Accessed: Aug. 20, 2024. [Online]. Available: https://www.ericsson.com/en/enterprise/curious/5g-campus-network.

[2] T. D. D. Et. al., “An Investigation and Analysis of Cyber Security Information Systems: Latest Trends and Future Suggestions,” Information Technology in Industry, vol. 9, no. 2, 2021, doi:10.17762/tii.v9i2.372.

[3] G. González-Granadillo, S. González-Zarzosa, and R. Díaz, “Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures,“ Sensors, vol. 21, no. 14, p. 4759, Jul. 2021, doi:10.3390/s21144759.

[4] J. M. A. Azmi Bin Mustafa Sulaiman, M. A. Abul Kairuddin, M. Rizal Mohd Isa, M. Nazri Ismail, M. Afzal Mohd Shukran, and A. Abu Bakar Sahaj, “SIEM Network Behaviour Monitoring Framework using Deep Learning Approach for Campus Network Infrastructure,” International journal of electrical and computer engineering systems, vol. 12, pp. 9–21, Nov. 2021, doi: 10.32995/ijeces.12.si12.

[5] I. Cvitić, D. Peraković, M. Periša, and S. Husnjak, “An Overview of Distributed Denial of Service Traffic Detection Approaches,” PROMET - Traffic&Transportation, vol. 31, no. 4, pp. 453–464, Aug. 2019, doi: 10.7307/vt.31i4.3082.

[6] G. A. Jaafar, S. M. Abdullah, and S. Ismaiel, “Review of Recent Detection Methods for HTTP DDoS Attack,” Journal of Computer Networks and Communications, vol. 2019, pp. 1–10, Jan. 2019, doi: 10.1155/2019/1283472.

[7] Fortinet, “What is a DDoS Attack? DDoS Meaning, Definition and Types,” Web. Accessed: Aug. 20, 2024. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/ddos-attack.

[8] A. Mishra, N. Gupta, and B. B. Gupta, “Defense mechanisms against DDoS attacks for accessibility in SDN-cloud using POX controller,” Telecommunications, vol. 77, no. 1, pp. 47–62, Jan. 2021, doi:10.1007/s11235-020-00747-w.

[9] Y. A. Bekeneva, “Algorithm for Generating Event Logs Based on Data from Heterogeneous Sources,” 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Jan. 2020, doi: 11.1093/eiiconrus49466.2020.903950.

[10] R. Ávila, R. Khoury, R. Khoury, and F. Petritello, “Use of Security Logs for Data Leak Detection: A Systematic Literature Review,” Security and Communication Networks, vol. 2021, pp. 1–29, Mar. 2021, doi:10.1155/2021/6615899.

[11] R. Ross, V. Pillitetti, and K. Dempsey, “Assessing enhanced security requirements for controlled unclassified information,” National Institute of Standards and Technology (U.S.), Mar. 2022, doi:10.6028/nist.sp.800-172a.

[12] E. Zagan and M. Danubianu, “Data Lake Architecture for Storing and Transforming Web Server Access Log Files,” IEEE Access, vol. 11, pp. 40916–40929, 2023, doi:10.1109/access.2023.3270368.

[13] A. Zola, “What is an access log?,” Web. Accessed: Aug. 20, 2024. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/access-log.

[14] A. AlSabagh and S. Kowalski, “A Framework and Prototype for A Socio-Technical Security Information and Event Management System (ST-SIEM),” 2016 European Intelligent and Security Informatics Conference (EISIC), Aug. 2016, doi:10.1109/eisic.2016.049.

[15] M. Schmidt, “Information security risk management terminology and key concepts,” Risk Management, vol. 25, no. 1, Dec. 2022, doi:10.1057/s41283-022-00108-8.

[16] MAMPU, “Cyber Security Framework For Public Sector (RAKKSSA),” PDF. Accessed: Aug. 20, 2024. [Online]. Available: https://www.malaysia.gov.my/portfolio/content/30090.

[17] Securities Commission Malaysia, “Guidelines on Management of Cyber Risk,” PDF. Accessed: Aug. 20, 2024. [Online]. Available: https://www.sc.com.my/api/document/download ashx?id=9aaddb2e-a413-409a-a47f-8d0124af6229.

[18] Technical Committee ISO/IEC JTC 1/SC 27, “ISO/IEC 27001 Information Security Management Systems,” Web. Accessed: Aug. 20, 2024. [Online]. Available: https://www.iso.org/committee/45306.html.

[19] A. Alfaadhel, I. Alhnomani, and M. Ahmed, “Risk-Based Cybersecurity Compliance Assessment System (RC2AS),” Applied Sciences, vol. 10, p. 6145, May 2023, doi:10.3390/app103116145.

[20] S. Ismaiel, N. M. Ismail, A. Ahmad, and M. A. Kairuddin, “Exploring the information security culture within industrial control systems organisations: Expert reviews,” VIII International Annual Conference “Industrial Technologies And Engineering” (ICITE 2021), 2022, doi:10.1063/5.0120877.

[21] M. F. Mustafa et al., “Student Perception Study on Smart Campus: A Case Study on Higher Education Institution,” Malaysian Journal of Computer Science, pp. 1–20, Dec. 2021, doi:10.22452/mjcs.v12i2.851.

[22] R. Rawia, M. R. M. Isa, N. M. Ismaila, A. A. B. Sajak, and A. Mustafa, “Preliminary study: Readiness of WLAN Infrastructure at Malaysian Higher Education Institutes to support Smart Campus Initiative,” JOIV : International Journal on Informatics Visualization, vol. 7, no. 3, pp. 945–951, Sep. 2023, doi: 10.30630/joiv.7.3.1242.

[23] A. S. Abdul Rahman, S. A. S. Ali, M. R. Is, F. Ali, D. Kamaruddin, and M. H. Baharuddin, “Performance Assessment of Malaysian Fossil Fuel Power Plants: A Data Envelopment Analysis (DEA) Approach,” International Journal of Renewable Energy Development, vol. 12, no. 2, pp. 247–260, Dec. 2022, doi:10.14710/ijred.2023.48487.

[24] J. V. Botello, A. P. Mesa, F. A. Rodriguez, D. Diaz-Lopez, P. Nespoli, and F. G. Marmol, “BlockSIEM: Protecting Smart City Services through a Blockchain-based and Distributed SIEM,” Sensors, vol. 20, no. 16, p. 4636, Aug. 2020, doi:10.3390/s20164636.

[25] B. Al-Duwairi, W. Al-Kahlia, M. A. Alrefai, Y. Abedalqader, A. Rawash, and R. Fahmawi, “SIEM-based detection and mitigation of IoT-botnet DDoS attacks,” International Journal of Electrical and Computer Engineering (IJECCE), vol. 10, no. 2, p. 2182, Apr. 2020, doi: 10.11591/ijecce.v10i2.2182-2191.

[26] H. Karlzén, “An Analysis of Security Information and Event Management Systems,” Chambers University of Technology, University of Gothenburg, no. January, 2009.

[27] J. Yadav, “Sentiment Analysis on Social Media,” Jan. 2023, doi:10.32388/y9x04.

[28] S. W. Kelley, C. N. Mhaonaigh, L. Burke, R. Whelan, and C. M. Gillan, “Machine learning of language use on Twitter reveals weak and non-specific predictions,” npj Digital Medicine, vol. 5, no. 1, Mar. 2022, doi: 10.1038/s41476-022-00576-y.

[29] A. Nistor and E. Zadobrischi, “The Influence of Fake News on Social Media: Analysis and Verification of Web Content during the COVID-19 Pandemic by Advanced Machine Learning Methods and Natural Language Processing,” Sustainability, vol. 14, no. 7, p. 10466, Aug. 2022, doi:10.3390/su141710466.

[30] R. Pandey et al., “A machine learning application for raising WASH awareness in the times of COVID-19 pandemic,” Scientific Reports, vol. 12, no. 1, Jan. 2022, doi:10.1038/s41598-021-03869-6.

[31] H. E. Che Hamid, N. A. Mat Razali, M. N. Ismail, M. A. Kairuddin, and M. R. Mohd Is, “A review paper: Forecasting of flood in Malaysia using machine learning,” VIII International Annual Conference “Industrial Technologies And Engineering” (ICITE 2021), 2022, doi: 10.1063/5.0116979.