ENHANCING CENTRALISED CYBERSECURITY FOR CAMPUS NETWORK INFRASTRUCTURE USING LOG CONSOLIDATION PROCESSING FRAMEWORK BASED ON SIEM

MOHD AZMI BIN MUSTAFA @ SULAIMAN

MASTER OF SCIENCE

UNIVERSITI PERTAHANAN NASIONAL MALAYSIA

2021

ENHANCING CENTRALISED CYBERSECURITY FOR CAMPUS NETWORK INFRASTRUCTURE USING LOG CONSOLIDATION PROCESSING FRAMEWORK BASED ON SIEM

MOHD AZMI BIN MUSTAFA @ SULAIMAN

Thesis Submitted to the Centre for Graduate Studies, Universiti Pertahanan Nasional Malaysia, in Fulfilment of the Requirements for the Master of Science

2021

ABSTRACT

One major problem commonly faced by network users is an attack on the security of the network especially if the network is vulnerable due to poor security policies. Network security is largely an exercise to protect not only the network itself but most importantly, the data. This exercise involves hardware and software technology. Secure and effective access management fall under the purview of network security. It focuses on threats both internally and externally, intending to protect and stop the threats from entering or spreading into the network. To address and ensure a secure network requires a complex combination of hardware devices, such as routers, firewalls with anti-malware software applications. Almost all agencies and companies use highly skilled information security analysts to implement security plans and regularly monitor the effectiveness of this plan. The main contribution of this research is to presents a significant and flexible way of providing centralised log analysis between network devices. To overcome these issues, this research proposes a new framework called Log Consolidation Processing (LCP) based on System Information Event Management (SIEM) technology. As a start, several frameworks based on System Information Event Management (SIEM) technology were studied for different environments. Next, two experiments to detect unauthorised access on external DNS Server and DDoS attacks were conducted to evaluate the effectiveness of the proposed framework. LCP managed to compile and display all potential threats and alert information in a single dashboard using a data mining approach for campus network infrastructure.

Keywords: SIEM, Network Behaviour Monitoring, Log Management, Campus Network Infrastructure

ABSTRAK

Salah satu masalah utama yang dihadapi oleh pengguna rangkaian adalah serangan terhadap keselamatan rangkaian terutama sekiranya rangkaian terdedah kerana dasar keselamatan yang tidak efisyen. Keselamatan rangkaian sebahagian besarnya adalah latihan untuk melindungi bukan sahaja rangkaian itu sendiri tetapi yang paling penting, data. Latihan ini melibatkan teknologi perkakasan dan perisian. Pengurusan akses yang selamat dan berkesan berada di bawah bidang keselamatan rangkaian. Ini memfokuskan pada ancaman yang baik secara dalaman atau luaran bagi tujuan untuk melindungi dan menghentikan ancaman dari dimasuki atau disebar ke dalam jaringan. Untuk menangani dan memastikan jaringan yang tersebut selamat, ia memerlukan kombinasi peranti perkakasan yang kompleks dan terjamin, seperti router, firewall dengan aplikasi perisian anti-malware. Hampir semua agensi dan syarikat menggunakan penganalisis keselamatan maklumat yang berkemahiran tinggi untuk melaksanakan rancangan keselamatan dan secara berkala memantau keberkesanan rancangan ini. Kajian penyelidikan ini mempelajari dan menggunakan cara yang signifikan dan fleksibel untuk menyediakan analisis log terpusat antara peranti rangkaian. Dalam penyelidikan ini, beberapa kaedah berdasarkan konsep *System Information Event and Management (SIEM)* telah dikaji dan dari kajian tersebut, kerangka baharu telah dicadangkan iaitu *Log Consolidation Processing (LCP)*. Secara ringkas, penyelidikan ini menjalankan dua eksperimen untuk menilai keberkesanan kerangka kerja yang dibangunkan. Lebih-lebih lagi, tujuan utama kerangka LCP ini dibangunkan bagi menyusun dan memaparkan semua potensi ancaman dan informasi waspada dalam satu dashboard menggunakan pendekatan perlombongan data untuk infrastruktur rangkaian kampus.

Kata kunci: SIEM, Pemantauan Tingkah Laku Rangkaian, Pengurusan Log, Infrastruktur Rangkaian Kampus

ACKNOWLEDGEMENTS

In the name of Allah SWT, the Most Merciful and Most Beneficent. Praise for giving me strength, opportunity, patience and blessing to complete this thesis.

I would like to express my gratitude to my Main Supervisor Dr Mohammad Adib bin Khairuddin and Co-Supervisor Dr Mohd Rizal bin Mohd Isa and Prof Dr Mohd Nazri bin Ismail for their constant encouragement, guidance and opinions throughout this thesis. May Allah bless them with happiness and external life.

My lovely mother and father Rohana bt Ibrahim and Mustafa @ Sulaiman bin Muhammad, thank you for all the sacrifices and love you have poured out so far. Who never tires of educating and giving the encouragement and support it deserves on this self. Thank you, mak and abah's services can't be answered.

Special thanks to my beloved wife, Nor Hafizah Zakaria, my children Nur Aina Darwisha, Nur Hanisah Nadhrah, Nur Fateena Izma, Muhammad Afiq Haikal, Nur Amna Nasuha and Muhammad Fattah Mukmin. Thank you so much for your love, patience, understanding, encouragement and full support throughout these years in completing my thesis.

Last but not least, my deepest appreciation goes to all my big family FMR in Johor and my friends who have given me ideas and comments.

APPROVAL

The Examination Committee has met on **17 August 2021** to conduct the final examination of **Mohd Azmi bin Mustafa @ Sulaiman** on his degree thesis entitled **Enhancing Centralised Cybersecurity for Campus Network Infrastructure Using Log Consolidation Processing Framework Based on SIEM.**

The committee recommends that the student be awarded the of Master of Science.

Members of the Examination Committee were as follows.

Prof. Ts. Dr. Omar bin Zakaria
Faculty Science and Defence Technology
Universiti Pertahanan Nasional Malaysia
(Chairman)

Prof. Madya Ts. Dr. Noor Afiza binti Mat Razali
Faculty Science and Defence Technology
Universiti Pertahanan Nasional Malaysia
(Internal Examiner)

Dr. Noor Zuraidin bin Mohd Safar
Fakulti Sains Komputer dan Teknologi Maklumat
Universiti Tun Hussein Onn Malaysia
(External Examiner)

APPROVAL

This thesis was submitted to the Senate of Universiti Pertahanan Nasional Malaysia and has been accepted as fulfilment of the requirements for the degree of **Master of Science.** The members of the Supervisory Committee were as follows.

Dr. Mohammad Adib bin Khairuddin
Faculty Science and Defence Technology
Universiti Pertahanan Nasional Malaysia
(Main Supervisor)

Dr. Mohd Rizal bin Mohd Isa
Faculty Science and Defence Technology
Universiti Pertahanan Nasional Malaysia
(Co-Supervisor)

Prof. Dr. Mohd Nazri bin Ismail
Faculty Science and Defence Technology
Universiti Pertahanan Nasional Malaysia
(Co-Supervisor)

UNIVERSITI PERTAHANAN NASIONAL MALAYSIA

DECLARATION OF THESIS

Student's full name : MOHD AZMI BIN MUSTAFA @ SULAIMAN

Date of birth : 07/07/1980

Title : ENHANCING CENTRALISED CYBERSECURITY FOR CAMPUS NETWORK INFRASTRUCTURE USING LOG CONSOLIDATION PROCESSING FRAMEWORK BASED ON SIEM

Academic session : 2020/2021

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

I further declare that this thesis is classified as:

☐ **CONFIDENTIAL** (Contains confidential information under the official Secret Act 1972)*

☐ **RESTRICTED** (Contains restricted information as specified by the organisation where research was done)*

☐ **OPEN ACCESS** I agree that my thesis to be published as online open access (full text)

I acknowledge that Universiti Pertahanan Nasional Malaysia reserves the right as follows.

i. The thesis is the property of Universiti Pertahanan Nasional Malaysia.
ii. The library of Universiti Pertahanan Nasional Malaysia has the right to make copies for the purpose of research only.
iii. The library has the right to make copies of the thesis for academic exchange.

Signature	**Signature of Supervisor/Dean of CGS/ Chief Librarian
Click here to enter text.	Click here to enter text.
IC/Passport No.	**Name of Supervisor/Dean of CGS/ Chief Librarian
Date:	Date:

*If the thesis is CONFIDENTAL OR RESTRICTED, please attach the letter from the organisation with period and reasons for confidentiality and restriction.
** Witness

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

FIGURE NO. **TITLE** **PAGE**

LIST OF ABBREVIATIONS

SIEM	Security Information and Event Management
OSSIM	Open Source Security Information Management
USM	Unified Security Management
DDoS	Distributed Denial of Services
IT	Information Technology
WAF	Web Application Firewall
IAM	Internet Access Management
IDS	Intrusion Detection System
SOC	Security Operation Center
SOCCs	Security Operation Control Center
Ext DNS	External Domain Name Servers
NGFW	Next Generation Firewall
PCI DSS standard	Payment Card Industry Data Security standard
APT	Advanced Persistent Threat
TTPDs	Techniques and Procedures Detection
TTPs	Techniques and Procedures
API	Application Programming Interface
AIS	Artificial Immune System

CHAPTER I

INTRODUCTION

1.1 BACKGROUND OF STUDY

Network security plays a critical part in Information Technology (IT). It is still difficult for organisations to meet security standards. Identity attacks, intrusions and hacking have been the most common security threats to the public and have also highlighted the importance of information security (Khan et al., 2017). By focusing on threats of both internal and external of the network, network security can secure and stop the threat from entering and spreading on the network. Ensuring a secure network requires a complex combination of hardware devices, such as routers, firewalls and anti-malware software applications.

In the campus network, all system and server equipment depends on the network administrator to collect logs of network equipment and servers, and also to monitor and notify the system status of the users. Therefore, it is important to have comprehensive centralised log management in the campus network. It is used to analyse events that occur from thousands of nodes to several dedicated servers where central analysis is carried out. When the analyses are obtained in a real-time process,

the safety events can be identified from the future events through event correlation and other advanced surveillance techniques. Moreover, it also can be an offline forensic activity, where past events are investigated to identify the occurrence of security that has taken place.

Aggregation of the data generated from multiple sources, identify specific threats and take appropriate action are the basic principles of each analysis of network and security reporting system. For instance, the system can take additional log information, generate alerts and ensure that all security controls can be monitored and prevented when such issues are detected. Log management infrastructure is a part of the hardware, software, networking and media used to generate, distribute, store, analyse and delete log data. Almost all organisations have one or more log management infrastructures.

Most organisations or businesses use the Security Information Event Management (SIEM) tool. This tool is used to streamline business compliance reporting via a centralised logging solution. Each host that is in use must have a log security record included in the report and can pass log data to the SIEM server. Single SIEM servers can collect log data from as many devices as they need and can produce a detailed report and manage all security events of each log they receive. In the current situation, each system needs to be able to manually retrieve data from each device regularly and to ensure that a central configuration of configuration can be generated to produce a report.

The SIEM system server is a tool for detecting unidentified events. Almost most of the equipment used does not comply with safety regulations and cannot track events or logs more deeply (Kołowrocki & Soszyńska-Budny, 2016). Although such

tools can identify and monitor events and produce audit log entries, they cannot analyse logins to detect unacceptable activities. Best of all, tools such as personal computers and laptops can alarm users when an event occurs. SIEM equipment can also perform higher detection by linking the events or logs of the equipment used. By collecting the events or logs of the linked equipment, the SIEM system can see attacks that have different angles on each of the different devices and can therefore record events or logs to decide if the attack is of nature and if it works.

SIEM equipment is used to improve the ability to manage any future accidents that can save time and money for incident handlers. The ability to deal with accidents rapidly and effectively will speed up the delay of occurrence, thus reducing the safety risk that cannot be followed by security events. SIEM equipment can also increase performance, mainly by offering a single report and review to display all security log data from many of the devices connected to it.

1.2 PROBLEM STATEMENT

I. Logs are scattered

It is very difficult to compile and view each event in the campus network and therefore, all logs in the campus network have been stored individually in their system. Few tools for log management, rather than performance and capabilities, are listed in random order (Agrawal & Makwana, 2015). Although threat detection platforms such as SIEM are significantly effective based on the recent reports that were found (Seyed & Seinali, 2016).

II. The high number of false-positive

Network administrators and the company network infrastructure monitoring are facing numerous tools which are not integrated (Filkins, 2019). Open standards are developed and maintained through a collaborative process that is consensus-driven to facilitate interoperability and the exchange of information between different products and services. Data related to incidents occurring in ICT security occurs less when compared to normal data. This will be the occurrence of a very unbalanced distribution when try to study the supervised model (Cinque et al., 2018).

III. Lack of context

For analysts, a solution needs to be created. It will not be meaningful if Syslog only pulls from the various data source. While it is not difficult to preserve the data collected with traditional methods such as hacking, it is an enormous challenge in an IoT environment to preserve the scene (Conti et al., 2018).

IV. Lack of support & expertise

Some logs can sometimes pose a massive difficulty. As a result, the agency needs to recruit dedicated staff to support the collection, analysis, correlation and normalisation of all the logs collected, or to retain time for the current team. The rapid growth of the campus network provides a challenge for IT staff to monitor and analyse the massive amount of data. Monitoring, maintaining, and expanding IT budgets 24/7. This means that the campus network must recruit professional staff or reserve the time of the current team to support the collection of data to detect, analyse, correlate and normalise all the logs collected. Researchers identified that the most frequently cited causes

for failure to achieve excellence in current SOCs are lack of skilled staff, budget and effective automation (Crowley & Pescatore, 2019).

1.3 RESEARCH QUESTIONS

Based on the problem statement, these are the research questions:

I. How does one study the network logs of a campus network?

II. How does one address the issues that occur during log monitoring exercises?

III. How do does one evaluate and measure the effectiveness of a proposed log monitoring framework?

1.4 OBJECTIVES

I. To study the current network infrastructure and analyse the particular raw log data of a campus network

II. To propose a framework for effective log monitoring through SIEM

III. To evaluate and measure the effectiveness of the proposed framework

1.5 RESEARCH SCOPE

The focus defines an area where SIEM is applied: This focus can be as narrow as needed as long as the primary process of the organization is present. In this research the focusses are as below:

- Focus on a specific tool to normalise, correlate and analyse:
    - SIEM (AlienVault)

- Next-Generation Firewall (NGFW)
- Web Application Firewall (WAF)
- Internet Access Management (IAM)

- Focus on two specific network attacks & detections experiments:
  - Unauthorised access
  - Distributed Denial of Service (DDoS) attacks
- The two experiments were conducted in the UPNMNet environment and infrastructure
- The specific data set collected for analysis are device logs, system logs, audit logs, database logs and application logs
- The duration for data collection is approximately three (3) to four (4) months to achieve a suitable number of data logs for analysis.

1.6 SIGNIFICANCE OF RESEARCH

- This research will provide a significant and flexible way of providing centralised log analysis between the security and network devices and how to display all threats alert information in a single dashboard.
- The system can assist the IT administrator to collect, store, analyse, investigate and report on the logs and other data for incident response, forensics and regulatory compliance purposes and analyse the event data in real-time to facilitate the early detection of targeted attacks, advanced threats and data breaches.
- To have an effective way of presenting the log file to the management.

1.7 THESIS OUTLINE

This research consists of five chapters namely Chapter 1: Introduction, Chapter 2: Literature Review, Chapter 3: Methodology, Chapter 4: Results and Discussion, and Chapter 5: Conclusion and Future Work.

- Chapter 1: Introduction

  This is an introductory chapter to the research, this chapter will discuss the introduction, problem statement, objectives, research scope and significance of the research.

- Chapter 2: Literature Review

  This chapter contains a literature review discussion that is related to this research.

- Chapter 3: Methodology

  This chapter will explain the methodologies that were used to carry out this research.

- Chapter 4: Results and Discussion

  This chapter will analyse the problem and requirement of this research and explore the area of interest in more depth to the research's objectives. Then it will explain and illustrate the two experiments used in this research, as a way to gauge the feasibility of the proposed framework. A brief discussion on the results and findings from the experiment will also be presented in this chapter.