Research and Implementation of Logstash in Network Security Event Analysis

Trần Ngọc Trung
Thai Nguyen University of Information and Communication Technology
Thai Nguyen University, Thai Nguyen, Vietnam
student655@ictu.edu.vn

***Abstract*—This undergraduate thesis investigates the deployment of Logstash as a core component of a Security Information and Event Management (SIEM) solution. The study begins by outlining the growing complexity of network threats and the necessity of real-time log analysis. A Docker-based ELK stack (Elasticsearch, Logstash, Kibana) is configured to receive logs from Windows and Linux hosts via Winlogbeat and Auditbeat, respectively. Logstash pipelines are defined to parse, enrich, and forward events to Elasticsearch, where Kibana visualizes them. The experimental environment demonstrates a configured collection route and example event views in a simulated setting. While no quantitative performance metrics are reported, the prototype confirms Logstash's suitability for rapid deployment in simulated network monitoring scenarios. The work highlights practical steps for integrating Logstash into existing security infrastructures and suggests directions for future research, including broader log sources and attack-simulation testing.**

***Index Terms*—Logstash, ELK stack, SIEM, network security, log analysis, Winlogbeat**

I. Introduction

Network security has evolved into a critical discipline, demanding continuous monitoring and analysis of diverse log streams. Traditional SIEM systems rely on efficient ingestion, parsing, and correlation of events to detect anomalies. Logstash, a flexible data processing engine, offers modular pipelines that can transform raw logs into structured formats suitable for downstream analytics. This thesis explores Logstash's role within an ELK stack, aiming to provide a lightweight yet powerful framework for event analysis. The objectives include: surveying the current state of network threat monitoring; detailing the lifecycle of security events; and demonstrating a practical deployment of Logstash to collect, process, and visualize logs from Windows and Linux hosts [1]. Earlier ICTU student work on related designs is included here for context [2], [3], [4], [5], [6], [7], [8]. Published technical books provide background for the methods discussed in this summary [9], [10], [11]. These contextual works were selected for this English summary; they are not asserted to appear in the original thesis bibliography.

II. Methods

The experimental setup employs Docker containers to host Elasticsearch, Logstash, and Kibana, ensuring isolation and reproducibility. Winlogbeat is installed on a Windows machine to harvest Application, System, Security, Sysmon, and PowerShell logs, while Auditbeat runs on a Linux host to capture audit events. Both beat agents are configured to forward logs to Logstash via the beats input on port 5044. Logstash pipelines are defined with input, filter, and output stages: the beats input receives agent events, filters transform selected fields, and the output stage forwards events to Elasticsearch. The manuscript reproduces configuration excerpts and interface screenshots. It does not include a separately versioned release package or a performance benchmark [1].

Supervisor: Nguyễn Anh Chuyên, Thai Nguyen University of Information and Communication Technology (nachuyen@ictu.edu.vn).

III. Results

The deployment successfully ingested logs from both Windows and Linux hosts into Elasticsearch. The manuscript shows Kibana views of collected events and describes the use of Windows and Linux log agents. It presents configuration and sample event screens rather than a measured throughput or loss analysis. These observations support the narrower conclusion that a simulated collection and visualization pipeline was assembled; they do not establish detection accuracy, resilience, or readiness for production monitoring [1].

IV. Discussion

The findings underscore Logstash's flexibility in integrating heterogeneous log sources into a unified SIEM pipeline. The thesis provides no throughput, latency, or resource benchmark, so scalability to enterprise traffic remains open. Future work should incorporate additional log types (e.g., firewall, web server, application logs) and simulate attack scenarios based on MITRE ATT&CK to assess correlation capabilities. Moreover, benchmarking resource consumption and latency would provide quantitative insights into deployment trade-offs [1].

V. Conclusion

This thesis presents a practical implementation of Logstash within an ELK stack for network security event analysis. By configuring Winlogbeat and Auditbeat to feed Logstash, the study demonstrates end-to-end log ingestion, processing, and visualization. The work contributes a documented experimental configuration that can be adapted to diverse environments. Subsequent research should expand log coverage, integrate complementary SIEM tools, and perform performance evaluations to guide large-scale adoption [1].

References

[1] Trần Ngọc Trung, ”Research and Implementation of Logstash in Network Security Event Analysis,” internal undergraduate thesis (original in Vietnamese), Thai Nguyen University of Information and Communication Technology, 2024.

[2] ICTU Student 102, ”Development of an Intrusion Detection System Based on Data Mining Techniques,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[3] ICTU Student 135, ”Construction of a Zigbee-Based Intrusion Detection System,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[4] ICTU Student 120, ”Development of a Simulation Program for Static Packet Filtering Firewall Technology,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[5] ICTU Student 129, ”Construction of a Network Security System for the Commercial Bank of Vietnam Hanoi Branch,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[6] ICTU Student 130, ”Construction of a Network Security System for a College of Education in Thai Nguyen,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[7] ICTU Student 105, ”Design of a Secure Network Using Cisco PIX Firewall for a Technical College,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[8] ICTU Student 106, ”Design and Security of Wi-Fi Networks for the Tai Nguyen Software Technology Center,” internal undergraduate thesis, Thai Nguyen University of Information and Communication Technology, 2009.

[9] J. Turnbull, The Logstash Book. Turnbull Press, 2013. ISBN 9780988820210.

[10] P. Shukla and S. Kumar, Learning Elastic Stack 7.0, 2nd ed. Packt Publishing, 2019. ISBN 9781789954395.

[11] A. Srivastava, Kibana 7 Quick Start Guide. Packt Publishing, 2019. ISBN 9781789804034.