Research Exhibition in Mathematics and Computer Sciences (REMACS 6.0)/
ISBN: 978-629-97440-5-4

THREAT HUNTING USING SECURITY ONION IN VIRTUAL NETWORK

Nur Maisarah Roslan, Mohd Faris Mohd Fuzi and Hafizah Hajimia
College of Computing Informatics and Mathematics,
Universiti Teknologi MARA, Perlis Branch
nmaisarah5009@gmail.com, farisfuzi@uitm.edu.my and hafizah.hajimia@uitm.edu.my

ABSTRACT- This project focuses on applying threat hunting, a proactive cybersecurity strategy, within a simulated network and systems. The objectives are to actively look for and identify sophisticated threats or malicious behaviors that could have sneaked past traditional security measures. The project adheres to a methodical threat hunting framework that includes phases like planning and preparation, hypothesis creation, data collection, analysis and continuous improvement. This project was conducted using Security Onion tools such as Sguil and Kibana. As a result, the threat hunting project has shown its effectiveness in proactively identifying and reducing threats, lowering the network's risk exposure, and maintaining a strong cybersecurity defense against constantly changing threats. The outcome of this project is expected to improve threat hunting skills, enhance security posture, and reduce the time spent in the presence of attackers in order to proactively deter emerging threats.

Keywords: Threat Hunting, Security Onion, Sguil, Kibana

1. INTRODUCTION

The research project has two main objectives which are to analyze activities and traffic across the simulated network while also aiming to identify possible anomalies also discover yet-to-be-discovered malicious activity using Security Onion tools like Sguil and Kibana. The scope of the project involves utilizing Security Onion tools to analyze network-based artifacts, with a focus on threat hunting operations for simulated attacks such as malware server and reconnaissance attacks. To evaluate the system's effectiveness in detecting and mitigating these threats, the project employs techniques such as observing network activity, examining system logs, and utilizing data visualization tools. The outcome of this project is expected to improve threat hunting skills, enhance security posture, and reduce the time spent in the presence of attackers in order to proactively deter emerging threats.

2. METHODOLOGY

This project's methodology takes a multi-step approach to identifying and analyzing threats. The project begins by collecting relevant network logs and data from a variety of sources, including bro_conn, bro_files, snort, and others. For real-time monitoring and analysis, these logs are then given into the Sguil and Kibana platforms. The analysis concentrates on two distinct attack scenarios: malware server assaults and reconnaissance attacks. The project makes use of the Sguil platform's advanced alerting features to find and look into suspicious activity connected to certain attack types. The data visualization tool Kibana is also used, enabling in-depth investigation of network traffic patterns and the detection of possible threats.

3. RESULTS AND DISCUSSION

Results of the project include IOC match visualizations, connections to network components, and assessments of their effects on the organization. The comparison table of highlighting the key differences between Sguil and Kibana are shown in Table 1.

Table 1 Key differences between Sguil and Kibana

Key	Sguil	Kibana
Purpose	Network security monitoring and analysis	Data visualization and exploration
Functionality	Real-time alerting of network events	Visualize, search, and analyze data stored
Data Sources	Network sensors	Log files, databases
Alerting	Advanced alerting capabilities	Built-in alerting features
Network Focus	Primarily focused on network security analysis	Can analyze various data types beyond network security

4. NOVELTY OF PROJECT

Over the years, a number of studies have used different methods to perform threat hunting. The current project and the project described in the article "An Efficient Approach of Threat Hunting Using Memory Forensics" (Danish et al, 2020), differ in their focus, methodology, and tools used. The implementation of Sguil and Kibana forms a crucial part of the current project, enabling real-time monitoring, alerting, and analysis. On the other hand, the article's project focuses on implementing the isolation forest algorithm for cyber threat hunting within a specific environment.

5. CONCLUSION

In conclusion, the combined use of Sguil and Kibana in the project allows for the detection, analysis, and response to simulated attacks. Sguil assists in the identification of suspicious activities and investigation of attacks, while Kibana's visualization capabilities enable better understanding of network traffic patterns, log data, and IOCs for improved situational awareness and proactive defense.

REFERENCES

Lukova-Chuiko, N., Fesenko, A., Papirna, H., & Gnatyuk, S. (2021). Threat Hunting as a Method of Protection Against Cyber Threats.

Stojkovski, B., Lenzini, G., Koenig, V., & Rivas, S. (2021). What s in a Cyber Threat Intelligence sharing platform? ACM International Conference Proceeding Series, 385–398. https://doi.org/10.1145/3485832.3488030

Whitman, M. E., & Mattord, H. J. (2019). 2019 Information Security Curriculum Development Conference: InfoSecCD '09, Kennesaw, GA, USA, September 25-26, 2019. ACM.