Cyprus University of Technology

Faculty of Engineering and Technology

Bachelor's Thesis

Application for making a more user-friendly intrusion prevention system (Suricata)

Stefanos Hannadjas

Limassol, May 2023

Cyprus University of Technology

Faculty of Engineering and Technology

Department of Electrical Engineering
Computer Engineering and Informatics

Application for making a more user-friendly intrusion prevention system (Suricata)

Stefanos Hannadjas

Limassol, May 2023

Approval Form

Cyprus University of Technology

Application for making a more user-friendly intrusion prevention system (Suricata)

Presented by

Stefanos Hannadjas

Advisor ______________________________

Dr. Michael Sirivianos

Cyprus University of Technology

Limassol, May 2023

Copyrights

The approval of the thesis by the Department of Electrical Engineering, Computer Engineering and Information does not necessarily imply the endorsement by the Department of the views of the writer.

Acknowledgements

I would like to express my gratitude to all those who shared their insightful experience and ideas and contributed to this paper. In particular, I would like to express my gratitude to Dr. Michael Sirivanos for his supervision and guidance throughout the thesis, from the approval and development of my idea to its completion. I would like to express my gratitude to Pantelitsa Leonidou for her helpful suggestions on how we can include user-friendliness in cybersecurity technologies. I would be remiss if I did not express my gratitude to Nikos Salamanos for his knowledge-sharing and technical assistance. Finally, I owe a lot to my family and friends who supported and encouraged me as I worked on my thesis.

Abstract

Undoubtedly, the internet has become an integral part of modern man, itself a source of knowledge for the construction of technologies that will bring automation and convenience to the lives of today's man. The internet is a double-edged sword. It can be used to facilitate our daily lives, but it can also be used for malicious actions. Nowadays, rapid growth has resulted in the continuous development of technologies. So every day, they are finding weaknesses in these technologies and, at the same time, developing various ways to do malicious actions. The present paper references the problem we are facing in modern society. The issue of inadequate security shielding in all age groups. The study was mainly based on creating an interface application for IPS systems to generate statistics in live time about risks that our IPS system faces. This paper focuses on the Suricata IDS/IPS tools, docker, and ELK stack so that the creation of the application other and quality security is explained. The general problem is essential, affecting organizations, companies and ordinary people. We experimented to see the efficiency of this work with many pcap file datasets to evaluate the application's performance and usability.